ISA

(Modules 1 to 6)

Background Material

INFORMATION SYSTEMS AUDIT 3.0 COURSE

Module - 2

Governance and Management of Enterprise Information Technology, Risk Management, Compliance & BCM Section

Digital Accounting and Assurance Board

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

Background Material
on
Information Systems Audit 3.0 Course

Module-2 :
Governance and Management of Enterprise Information Technology, Risk Management, Compliance & BCM Section

Digital Accounting and Assurance Board
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Revised Edition	:	August, 2020
Committee/Department	:	Digital Accounting and Assurance Board
Email :		gdaab@icai.in
Website :		www.icai.org/ https://pqc.icai.org
Price	:	₹ 750/- (For Complete Set)
ISBN	:	978-81-8441-995-5
Published by	:	The Publication Directorate on behalf of The Institute of Chartered Accountants of India ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110002
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra – 282 003 August | 2020 | P2724 (Revised)

Foreword

The digital revolution is transforming the traditional ways of doing business, necessitating realignment of profession to leverage the multipliers of digital technology - enhanced efficiency, scale and speed, effectiveness, agility and giving access to newer markets. In view of the rapid technological changes, it is imperative for Information System Auditors to adapt, be innovative in aiding organizations to improve its control environment and strengthen governance of IT risks. Adoption of emerging technologies will help them to assimilate vast amount of data and provide value added analysis in the form of data analysis and business intelligence. Chartered Accountants possess unique blend of systems and process understanding and expertise in controls and governance, thereby best suited to be the perfect Information Systems Auditor.

The Institute of Chartered Accountants of India (ICAI), through its Digital Accounting and Assurance Board (DAAB), is continuously monitoring technological developments and taking initiatives to disseminate updated knowledge amongst our members and other stakeholders. In this direction, it is heartening to note that the DAAB is bringing out next version of "Educational Material" for Post Qualification Course on Information Systems Audit. This updated and revised Material combines technology, information assurance and information management expertise that enable Chartered Accountants to be an advisor and handling assurance assignments.

In this updated course curriculum various aspects of emerging technologies like, Blockchain, Robotics Process Automation, etc., have also been introduced to keep members fully abreast. With focus on increased practical aspects, case studies and lab manuals at appropriate places this material is a great learning guide for members aspiring to be Information Systems Auditor.

I compliment CA. Manu Agrawal, Chairman, CA. Dayaniwas Sharma, Vice-Chairman and other members of the Digital Accounting and Assurance Board for generation next material in digital era by taking up this timely initiative.

I am confident that our members would take benefit of these updated modules of post qualification course on Information Systems Audit, so as to render their professional responsibility as Information System Auditor more efficiently and highest standards to achieve global recognition.

CA. Atul Kumar Gupta

President, ICAI

Place: New Delhi

Date: April 12, 2020

Preface

Evolution of digital economy and ever changing dynamic ecosystem presents significant challenges, including new competition, new business and service delivery models, unprecedented transparency, privacy concerns and cyber threats. With a goal to keep members abreast of impact of emerging technologies, Digital Accounting and Assurance Board has come out with the updated Post Qualification Course on Information Systems Audit Modules to equip members with specialised body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilize and leverage technology to provide reasonable assurance that an organization safeguards it data processing assets, maintains data integrity and achieves system effectiveness and efficiency. This updated syllabus facilitates high level understanding about the role and competence of an IS Auditor to analyse, review, evaluate and provide recommendations on identified control weaknesses in diverse areas of information systems deployment.

Revised Modules of Post Qualification Course on Information Systems Audit has specific objective, i.e., "To provide relevant practical knowledge and develop skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance of Information Systems." The core of DISA 3.0 lies in inculcating competence to add to service delivery of the members. The updated course would help the members to apply appropriate strategy, approach, methodology and techniques for auditing information system and perform IS Assurance and consulting assignments by using relevant best practices, IS Audit standards, frameworks, guidelines and procedures.

The updated ISA Course 3.0 has a blend of training and includes e-learning, live case studies and lab manuals, project work in addition to class room lectures. This updated background material also includes a DVD which has e-Learning lectures, PPTs, case studies, DEMO CAAT software, useful checklists and sample audit reports. New Module on "Emerging Technology and Audit" has been added which covers Information System Assurance and Data Analytics, Assurance in Block chain Ecosystem, and Embracing Robotic Process Automation in Assurance Services. In addition to this Artificial Intelligence and Internet of Things (IoT) has also been inducted in the new modules.

We would like to take this opportunity to place on record our deep appreciation for the efforts put in by Convener, Dr. Onkar Nath as well as authors and reviewers of the various modules, viz., CA Anand Prakash Jangid, Mr. N.D. Kundu, Mr. Inder Pal Singh, Mr. Avinash Gokhale, CA Pranay Kochar, CA Naresh Gandhi, Dr Manish Kumar Srivastava, Dr. Saurabh Maheshwari, CA Narasimhan Elangovan and CA Atul Kumar Gupta. It would be also appropriate to express our thanks to all the ISA faculties for giving their inputs/ suggestions for the implementation of DISA 3.0.

We would like to express gratitude to CA. Atul Kumar Gupta, President, ICAI, and CA. Nihar Niranjan Jambusaria, Vice President, ICAI, for their thought leadership and encouragement to the initiatives of the Board. We would also like to place on record our gratitude for all the Board members, co-opted members and special invitees for providing their valuable guidance and support in this initiative of the Board. We also wish to express my sincere appreciation for CA. Amit Gupta, Secretary, DAAB, Ms. Nishi Saraf, Section Officer for their untiring efforts in finalization of the updated Modules.

We are sure that these updated Modules on Post Qualification Course on Information Systems Audit would be of immense help to the members and enable them to enhance service delivery not only in compliance, consulting and assurance of IT services, but also provide new professional avenues in the areas of IT Governance, Cyber Security, Information System Control and assurance services.

CA. Manu Agrawal
Chairman
Digital Accounting and Assurance Board

CA. Dayaniwas Sharma
Vice-Chairman
Digital Accounting and Assurance Board

Contents

Chapter 1

Concepts of Governance and Management of Information Systems

Learning Objective

Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.

1.1 Introduction

The need for governance and management of information systems can be assessed from the simple fact that today technology is all pervasive. Organizations are so dependent on Technology that its failure will bring all key operations to a complete halt. On the positive side, technology facilitates organizations to offer products or services to anyone across the globe. The fundamental principle in the current business environment is to use technology to enable users to access information anytime, anywhere, anyhow by anyone. The objective is to provide information access to all stakeholders online with real-time access and update. This is done using enabling technology such as the network, Internet, hardware, operating system software, database, applications and browser. Modern Technology is empowered by the cloud and internet access through wireless broadband. Technology is only an enabler but the backbone for this has to be robust systems and processes for the information systems. Hence, it is critical to ensure that organizations embed Governance and management processes and other enablers in the technology deployed. This will ensure that various stakeholder requirements are met and the management at all levels are able to use technology to perform their responsibilities. It is important to comply with the requirements of corporate governance or enterprise governance by implementing Governance of Enterprise IT, enterprise risk management using appropriate risk management strategy and internal control systems. This chapter outlines these concepts and provides overview of how to implement EGIT

1.2 Key Concepts of Governance

Enterprises whether they are commercial or non-commercial, exist to deliver value to their stakeholders. Delivering value is achieved by operating within value and risk parameters that are acceptable and advantageous, and by using resources including IT responsibly. In the rapidly changing environment that most enterprises operate in, swift direction setting and agility to change are essential. Senior management is responsible for ensuring that the right structure of decision-making accountabilities is shared among many people in the enterprise and when accountability is shared, governance comes into play. Governance is “the

combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives." Governance should be in place to ensure IT supports the strategies and objectives of the organization. The relationship of enterprise Governance and Corporate Governance with IT governance (EGIT is depicted below)

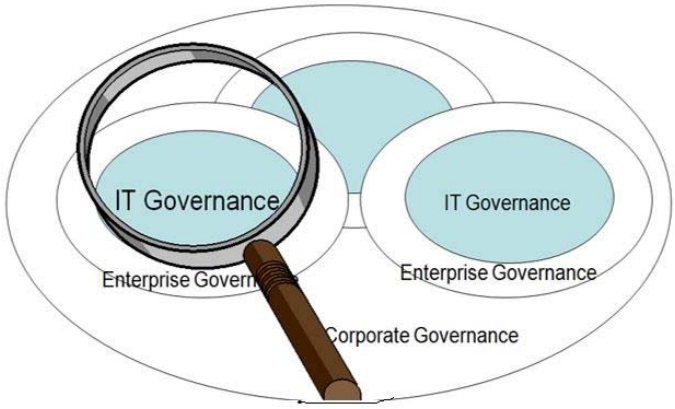

Figure 1.1: Relationship of types of Governance

1.2.1 Enterprise Governance

ISO/IEC 38500 defined Governance as: "The system by which organisations are directed and controlled". A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives. Enterprise governance can be defined as: 'The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.' Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit. Examples include codes on corporate governance and financial reporting standards.

The key message of enterprise governance is that an organisation must balance the two dimensions of conformance and performance needs to ensure long-term compliance and success. This requires that governance is ideally implemented with the right balance of conformance and performance dimensions. These two dimensions are briefly outlined here.

1.2.2 Conformance or Corporate Governance Dimension

The conformance dimension of governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: roles of the chairman and

CEO, role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance. Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee or its equivalent in countries where the two-tier board system is the norm. Other committees are usually the nominations committee and the remuneration committee. The Sarbanes Oxley Act of US is an example of providing for such compliances from conformance perspective.

1.2.3 Performance or Business Governance Dimension

The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward-looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required. The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. There is thus an oversight gap in respect of strategy. One of the ways of dealing with these lacunae is to establish a strategy committee of similar status to the other board committees which will report to the board. The performance dimension in terms of how to implement performance management system is covered in more detail in chapter 4 of this module.

1.2.4 Enterprise Governance Framework

Enterprise governance in general is broader and encapsulates corporate governance, performance management, internal control and enterprise risk management. In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. The objective of implementing enterprise governance is to ensure that the governance objectives of benefits realisation, risk optimisation and resource optimisation are achieved considering the stakeholder needs and which leads to value creation for the enterprise. This is depicted in the figure 1.3 given here.

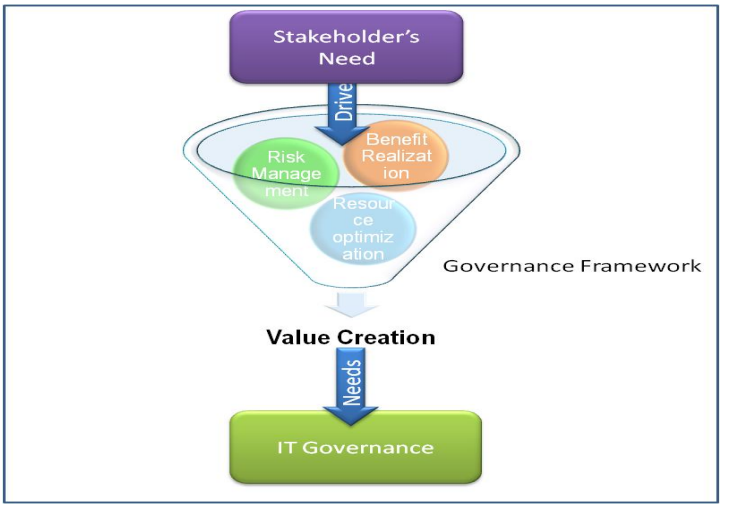

Figure 1.2: IT Governance framework and Drivers

1.2.5 Corporate Governance

Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business by ensuring compliance and protecting shareholders' interest.

Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of audit committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. These are intended to guide companies to achieve their business objectives in a manner such that those who are entrusted with the resources or power to run the companies to meet stakeholder needs without compromising the shareholders' interest. Legally, the directors of a company are accountable to the shareholders for their actions in directing and controlling the business, and for the actions of the company's employees, who are in the position of trust to discharge their responsibilities in the best interest of the company. Corporate governance is thus necessary for the purpose of monitoring and measuring their performance and is mandated by regulations across the world and across various industries.

Figure 1.3: Corporate Governance Participants

1.2.6 Need for Corporate Governance

Although Governance is not new for enterprises, a spate of frauds in the corporate sector involving large enterprises across the world including India in the last two decades have awakened regulators to the need for mandating the implementation of corporate governance integrated with Enterprise Risk Management and Internal controls. The concept of Corporate Governance has succeeded in attracting a great deal of public interest because of its importance for the economic health of companies, protecting the interest of stakeholders including investors and the welfare of society, in general.

Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, management, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. The requirements for corporate governance are built on the principles of governance and encompass all levels of management including specific responsibility of board and senior management. Corporate Governance is focused on protecting the interests of various stakeholders and is compliance oriented. Although the terms corporate governance and enterprise governance are quite often used inter-changeably, it can be said that corporate governance is applying the principles of enterprise governance to corporate structure of enterprises. Some of the key concepts of corporate governance are:

- Clear assignment of responsibilities and decision-making authorities, incorporating a hierarchy of required approvals from individual employees to the board of directors;
- Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;
- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. vendors);
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

1.3 Corporate Governance and Regulatory Requirements

Corporate governance in India is evolving, primarily due to regulatory requirements, but also, to some extent, due to each enterprise's specific needs and context. The objectives of corporate governance are fulfilled by setting up an appropriate structure and functioning mechanisms for the board of directors and audit committees, as laid down by the Companies Act, 2013.It is critical for each enterprise to establish its own specific governance system based on its own specific constraints and business culture.

The Companies Act, 2013 outlines the need for mandatory Internal Audit and reporting on Internal Financial Controls [sections 138]. The Act requires certain new aspects which need to be covered in an auditors' report which include: "whether the company has adequate internal financial controls system in place and the operating effectiveness of such controls [section 143(3) (i) of the 2013 Act]. The Board of Directors are responsible for governance of their companies. SEBI introduced a mandatory audit to ensure that this is maintained as per its norms by all listed companies as part of corporate governance.

Further, the Act deals extensively on the issue of fraud (section 447) and has for the first-time defined fraud. The new regulations make it more imperative for management to implement a system of governance integrated with risk management and internal control systems. As IT is a key enabler of enterprise processes, risk management and controls has to consider technology and hence the need for implementing a holistic approach of Enterprise

Governance of Information and Technology (EGIT) using global best practices and frameworks.

The Information Technology Act amended in 2008 introduced new provisions which are specifically applicable to corporates, provisions relating to maintaining privacy of information and imposed compliance requirements on management with penalties for non-compliance. These requirements have to be considered as part of compliance by corporates and individuals as applicable.

In the US, The Sarbanes Oxley Act (SOX) focuses on the implementation and review of internal controls as relating to financial audit. It highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented in the relevant computerised information systems. The overall reliability of these controls would be dependent on the overall risk management strategy, risk appetite of the management, use of best practices and various other enablers.

Corporates across the world for SOX compliance have used COBIT 2019 (www.isaca.org/COBIT 2019) as the primary framework and best practices for implementing governance, risk management and internal controls. COBIT 2019 is a comprehensive framework for the governance and management of enterprise I&T, comprising five domains, 40Governance and Management objectives and over 200 management practices and activities divided into governance and management managed processes. Cobit 2019 has been discussed in detail in subsequent chapters of this module.

Good corporate governance is vital for all types of enterprises big or small in view of the benefits which accrues due to its implementation. Governance helps in ensuring that control failures are mitigated appropriately. However, good corporate governance on its own cannot make an organisation successful. There is a danger that insufficient attention is paid to the need for organisations to create wealth or stakeholder value. Strategy and performance are also important.

1.4 Enterprise Governance of Information and Technology (EGIT)

Enterprise Governance of Information and Technology is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of EGIT are to analyse and articulate the requirements for the governance of enterprise IT, establish and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives. The key benefits of using EGIT is that it provides a consistent approach integrated and aligned with the enterprise governance approach. It ensures that IT-related decisions are made in line with the enterprise's strategies

and objectives and the IT-related processes are overseen effectively and transparently.

Implementing a EGIT framework helps in better compliance with legal and regulatory requirements and ensures that the governance requirements for board members are met. A few decades back, IT was one of the wagons but now IT is the engine propelling enterprise growth. IT interfaces all aspects of the enterprise and not just transaction processing. It can be said that IT has become inseparable from the business. Hence, in a modern enterprise, IT has moved from being a mere service provider to a strategic partner which helps enterprises in achieving both competitive and strategic advantage. Considering this huge dependence on IT and the fact that internal controls are embedded in IT and effective risk management can be achieved by using IT, implementing Governance of Enterprise IT has become imperative for a modern enterprise. Regulatory agencies, professional bodies and associates issue guidelines on use of generic and specific best practices. For example, the Reserve Bank of India issues guidelines covering various aspects of secure technology deployment. These guidelines are prepared based on various global best practices such as COBIT 2019 and ISO 27001. The Information technology Rules, 2011 outlines the need for maintaining secrecy of personal and sensitive information and identifies ISO 27001 as “Reasonable Security Practices and Procedures” for implementing best practices.

1.4.1 Implementing EGIT

Enterprise Governance of Information and Technology is built on the principles of Governance but applied to IT. Hence, implementing EGIT in organizations requires understanding concepts of Governance, IT deployment and how IT can be used to implement Governance. EGIT is a blend of these concepts. Implementing EGIT requires establishing the right structures with defined roles and responsibilities, implementing relevant processes using best practices as required and establishing the relational mechanisms by active participation of relevant stakeholders as required in a collaborative effort to achieve enterprise goals.

The improvement of governance of enterprise IT is increasingly recognized by top management as an essential part of enterprise governance. Effective EGIT will result in improved business performance as well as compliance to external requirements, yet successful implementation remains elusive for many enterprises. Effective EGIT requires a range of enablers with carefully prescribed roles, responsibilities and accountabilities that fit the style and operational norms specific to the enterprise. Implementing EGIT from conformance (corporate) perspective would require viewing the enterprise at macro level and consider not only the business but also the external linkages. In case of performance (business) the enterprise has to be viewed at internal level and the focus on the processes and activities within the enterprise.

The key areas of focus in implementing EGIT are summarized in the table here.

Table 1.1: Implementing Governance from Conformance or performance perspective

Area	Conformance (Corporate)	Performance (Business)
Scope	• Board Structure, Roles and Remuneration	• Strategic decision making and value creation
Addressed via	• Standards and Codes	• Best practices, tools and techniques
Auditability	• Can be audited for compliances	• Not easily auditable
Oversight Mechanism	• Audit Committee	• Balance score cards

The COBIT 2019 framework can be used for implementing EGIT from any/both the above perspectives. The seven key components of EGIT which are required for effective implementation are described in further chapter. Overall, EGIT requires structures, processes and relational mechanisms.

The components and relationship of IT Governance framework are outlined in figure given below.

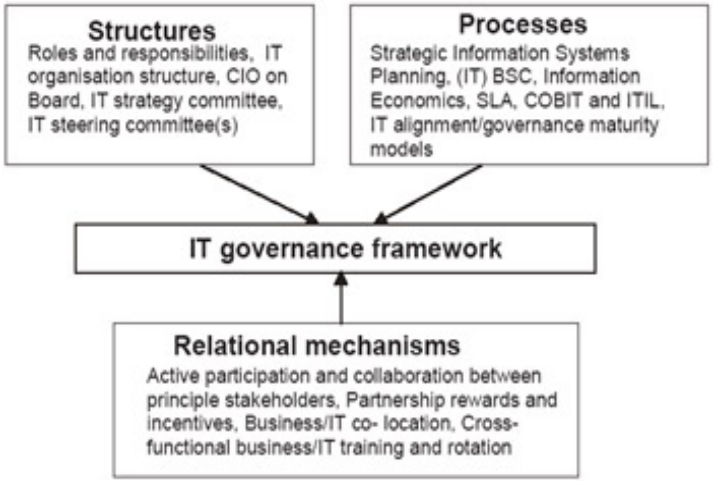

Figure 1.4: Components of Governance Framework

The structures involve the organization, and location of the IT function, the existence of clearly defined roles and responsibilities and a diversity of IT/ business committees. The processes refer to strategic decision making, strategic information systems planning (SISP) and monitoring, control, and process frameworks. The relational mechanisms finally complete the governance framework and are critical for attaining and sustaining business-IT alignment, even when the appropriate structures and processes are in place. These mechanisms include business/IT participation, strategic dialogue, training, shared learning, and proper

communication. COBIT 2019 which is the business framework for implementing EGIT can be used by enterprises of all sizes and types and regardless of technology deployment.

1.4.1.1 Guidelines for Implementing EGIT

The primary objective of implementing EGIT is to ensure IT delivers value to the business and helps in mitigation of IT-related risk. This is enabled by the availability and management of adequate resources and the measurement of performance to monitor progress towards the desired goals. The COBIT 2019 implementation guide provides a systematic approach with defines phases and specific roles and responsibilities for implementing EGIT. This approach can be customized and used by any organization regardless of size, nature of business, sector or technology used.

1.4.1.2 Systemic Approach to Implementing EGIT

Research studies have established that effective implementation of EGIT maximizes the contribution made by IT to organizational success. There can be multiple approaches to implementing EGIT as this varies with the needs of the enterprise and the specific framework used. It is advisable to adapt a systematic and well-proven approach as outlined in some of the best practices and frameworks. IT solution providers and regulators also provide their own approaches for implementing EGIT. It is important to remember that the focus should be first on implementing the systems and processes first and then automating rather than expecting that automation will implement systems and processes as required. As explained earlier, frameworks such as COBIT 2019 also provide a systematic approach for implementing the relevant frameworks. The technology and business frameworks can be easily integrated under these frameworks. We are giving below some general guidelines on implementing EGIT which can be adapted as required.

1. Aligning IT Goals with Business Goals

Achieving better governance starts with the business, and more specifically with understanding its strategy and goals. IT management should be involved early in the business strategy definition process, especially in those companies that are highly dependent on IT. The IT goals should be aligned to the business goals. The IT strategy should be an IT blueprint of the business strategy plan. The IT goals set out in the IT strategy plan should clearly support the achievement of one or more business goals. It is the responsibility of the board and senior management to ensure that the IT strategy is aligned with the business strategy. This could be achieved through:

- Clear business goals, communicated to the entire organisation
- Early involvement of IT in business strategy process
- Align IT goals to business goals
- Derive IT strategy from business strategy

2. Formalise and Implement Right IT Governance Processes

After aligning the IT goals with the business goals, it is important to implement required set of efficient and effective IT governance and management processes. Using best practices such as COBIT 2019 will facilitate such implementation. It is important to select the most critical process based on business priorities, assign process owners, develop metrics and monitor the achievement of process as per set objectives.

3. Establish Required IT Organisation and Decision Structure

Effective Governance of enterprise IT is determined by the way the IT department is organised and where the IT decision-making authority is located within the organisation. The responsibility for governance rests with the board of directors as they are responsible for evaluating, directing and monitoring the governance processes as per stakeholder requirements. They have to establish the right management structure with the C suite to ensure there is proper collaboration between business and IT department.

4. Involve Board of Directors/Executive Management in IT Related Matters

Governance initiatives may be initiated by IT or internal auditors but the overall responsibility vests with the board who assign specific responsibility to senior management from both business and IT. The executive management has to be aware and actively participating in the existing governance activities. IT topics and decisions should regularly appear and be discussed in executive committees or on-board level, especially in organisations where IT plays a crucial role in keeping the business running. Even when the CIO is not a part of the executive committees, he should be represented by another executive member or he/she could be invited whenever an IT related topic is handled.

5. Govern and Manage Roles and Responsibilities

The board should ensure that governance and management structures are established involving the organisation, the location of the IT function, the existence of clearly defined roles and responsibilities and a diversity of IT/business committees. The organisation structure should specify clear responsibilities defined towards the business they work for, and this throughout all levels, including the CIO and IT management. To make sure individuals adopt and execute upon their roles and responsibilities, a process of 'formal' evaluation and regular process of review has to be implemented as part of performance management system.

6. Establish IT Strategy and IT Steering Committee

Effective committees created at the right level with clearly defined roles and responsibilities play an important role in establishing ensuring alignment of IT with business which is key to successful implementation of EGIT. IT strategy committee has to operate at the board level and the IT steering committee has to operate at executive level with each committee having specific responsibility, authority and membership. The roles and responsibilities of these two key committees are explained in later chapter of this module.

7. Plan, Align and Manage IT Enabled Investment as a Portfolio

Successful implementation of EGIT requires organisation to effectively their IT enabled investments throughout the economic life cycle of the projects using best practices of project management as required. Clear responsibility has to be allocated between IT who would be responsible for execution of IT enabled projects, but business has to be responsible for analysing the anticipated benefits and making decisions.

8. Implement Performance Measurement System Integrated with Regular Process

Measuring and monitoring the different IT processes at different levels is very important to review whether the set required service levels are met as set by the functional management. Goals have to be set at each of the levels starting from activity to process and linked to IT goals which are in turn linked to business goals. Metrics have to be set and monitored to ensure implementation and corrective action has to be taken as required. The performance management system could be integrated using the balanced scorecard technique with the complete set of metrics which is consolidated for different levels and areas as required. This is explained in detail in chapter 4.

9. Establish Sustainability Through Support, Monitoring and Regular Communication

IT is most important support function to business activities as most of the service now a days are delivered through IT. Aligning business goals with IT goals requires ongoing and constant interaction between IT and business function. There has to be effective collaboration and interaction between business and IT. This requires a constant communication channel and mechanism to encourage the relationship between business and IT.

1.5 Enterprise Risk Management

Enterprise risk management deals with risks and opportunities affecting value creation or preservation and is defined by the Institute of Internal Auditors as: “Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” The management to ensure that the enterprise risk management strategy considers information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise

1.5.1 Governance Objectives

It is important to identify specific governance objective in implementing EGIT. Generally, the focus area of implementing EGIT as specified in COBIT 2019 are these are the governance objectives:

- Benefit Realisation: Creating new value for the enterprise through I&T, maintaining

and increasing value derived from existing I&T investments, and eliminating IT initiatives and assets that are not creating sufficient value for the enterprise. The basic principles of I&T value are delivery of fit-for-purpose services and solutions on time and within budget and generating the financial and nonfinancial benefits that were intended. The value that I&T delivers should be aligned directly with the values on which the business is focussed and measured in a way that transparently shows the impacts and contribution of the I&T-enabled investments in the value creation process of the enterprise.

- Risk Optimisation: Addressing the business risk associated with the use, ownership, operation, involvement, influence and adoption of I&T within an enterprise. I&T-related business risk consists of I&T-related events that could potentially impact the business. While value delivery focuses on the creation of value, risk management focuses on the preservation of value. The management of I&T-related risks should be integrated within the enterprise risk management approach to ensure a focus on IT by the enterprise and be measured in a way that transparently shows the impacts and contribution of I&T-related business risk optimisation in preserving value.
- Resource Optimisation: Ensuring that the right capabilities are in place to execute the strategic plan and sufficient, appropriate and effective resources are provided. Resource optimisation ensures that an integrated, economical IT infrastructure is provided, new technology is introduced as required by the business, and obsolete systems are updated or replaced. It recognises the importance of people, in addition to hardware and software, and, therefore, focuses on providing training, promoting retention and ensuring competence of key IT personnel.

1.5.2 Internal Controls

Regulatory requirements and reasonable practices framework require internal control system to be an integral part of enterprise risk management and governance system. Hence, it is important to understand how internal control requirements are generally implemented through management systems. “An effective internal control system is an essential part of the efficient management of a company” established through the governance system. Such systems should establish an adequate system of internal control to “support business requirements for effective and efficiency of operations, reliability of information and compliance with laws and regulations.” While appropriate internal control is a required outcome of sound governance and a necessary supporting element of effective governance, it does not in itself represent governance.

Any audit whether it is compliance or IS oriented would require understanding of internal control system implemented within the enterprise. Internal control is an element of the management system rather than an aspect of the governance system. Internal control must be

supported by effective risk management process with internal control arrangements determined by the enterprises level of risks. Risk management requires establishing a sound system of risk oversight and management and internal control. The Securities and Exchange Commission (SEC) of USA rules define "internal control over financial reporting" as a "process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company;
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Figure 1.5: Process of Internal Control

Implementing internal controls systems is imperative for effective governance both from regulatory and management perspective. As auditors are primarily control experts, they can review the availability, adequacy and appropriateness of implemented controls and provide appropriate recommendations for mitigating control weaknesses. IS Auditors may be required to review and evaluate the system of governance, risk management and controls as

embedded in IT and information systems and provide assurance on the effectiveness to meet established objectives.

1.6 Summary

This chapter has provided an overview of concepts and practice of various aspects of Governance such as enterprise governance, corporate governance and EGIT. The interfaces between the different levels at which governance is implemented have also been highlighted. As IT is a key enabler of organization processes, it is critical to implement EGIT as an integral part of governance. The regulatory and management requirements for implementing governance start with clearly established objectives and require using a systematic approach and use of relevant best practices frameworks as required. Corporate Governance and EGIT are closely inter-linked with enterprise risk management and internal controls. Regulatory requirement mandates the implementation of governance, enterprise risk management and internal controls. Organizations are established with the objective of value creation. Hence, they will implement governance not only from conformance perspective but also to provide value to the organization. Hence, the two dimensions of conformance and performance have to be balanced in implementing governance in enterprises. Guidelines for implementing EGIT have been explained through a generic guideline starting from aligning IT strategy with enterprise strategy and ending with ensuring sustainability of EGIT implementation and thus making it an integral part of day to day process.

1.7 Questions

1. Who is responsible for establishing right structure of decision-making accountabilities?
   - A. Senior management
   - B. Operational management
   - C. Chief information officer
   - D. IT steering committee
2. The MOST important benefit of implementing Governance of Enterprise IT is:
   - A. Monitor and measure enterprise performance
   - B. Provide guidance to IT to achieve business objectives
   - C. Run the companies to meet shareholders' interest
   - D. Ensure strategic alignment of IT with business
3. The primary objective of Corporate Governance is:
   - A. Reduce IT cost in line with enterprise objectives and performance.
   - B. Optimise implementation of IT Controls in line with business needs

C. Implement security policies and procedures using best practices.

D. Increase shareholder value by enhancing economic performance.

4. The ultimate objective Governance of Enterprise IT is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of:

A. Shareholders

B. Stakeholders

C. Investors

D. Regulators

5. Which of the following is a key component of Corporate Governance?

A. Employee rights

B. Security policy

C. Transparency

D. Risk assessment

6. Effective Governance of Enterprise IT requires processes to ensure that:

A. risk is maintained at a level acceptable for IT management

B. the business strategy is derived from an IT strategy

C. IT governance is separate and distinct from the overall governance

D. the IT strategy extends the organization's strategies and objectives.

7. Business Governance helps the Board by enabling them to understand:

A. enterprise functions

B. risk assessment

C. key performance drivers

D. Key controls

8. The effectiveness of the IT governance structure and processes are directly dependent upon level of involvement of

A. Heads of Business units

B. Internal auditor department

C. Technology management

D. Board/senior management

9. Which of the following is one of the key benefits of EGIT?

A. Identification of relevant laws, regulations and policies requiring compliance.

B. Improved transparency and understanding of IT's contribution to business

C. Better utilization of human resources by using automation

D. Increased revenues and higher Return on investments.

10. Which of the following is the primary objective for implementing ERM?

A. Implement right level of controls.

B. Better availability of information.

C. Tighter security at lower cost.

D. Implement IT best practices.

1.8 Answers and Explanations

1. A. The senior management is responsible for ensuring right structure of decision-making accountabilities. The operational management is responsible for ensuring that operations of the enterprise are run as per enterprise policy. The chief information officer is responsible for ensuring IT enabled investments provide business value and the IT steering committee is responsible for steering IT enabled projects toward successful completion of objectives.

2. D. The MOST important benefit of implementing Governance of Enterprise IT is that it helps in ensuring strategic alignment of IT with business. Alignment of IT strategy in tune with enterprise strategy ensures value delivery from IT enabled investments. The monitoring and measuring of enterprise performance is one of the key processes of EGIT. EGIT does not provide guidance to IT to achieve business objectives but provides overall framework and setting for IT to achieve business objectives. Although EGIT is often implemented from a regulatory perspective and enables enterprises to meet corporate governance requirements, it does not directly focus on running the enterprises based on shareholders' interest. Shareholders are one of the key stakeholders whose objectives are considered while formulating enterprise goals.

3. C. The primary objective of Corporate Governance is increasing shareholder value by enhancing economic performance. Reducing IT cost in line with enterprise objectives and performance is not an objective. Further, optimise implementation of IT Controls in line with business needs has to be considered as part of EGIT and is not directly objective of corporate governance. Implementing security policies and procedures using best practices is not the primary objective of corporate governance.

4. B. The ultimate objective Enterprise Governance of Information Technology (EGIT) is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of the stakeholders. There are multiple stakeholders and EGIT requires balancing the needs of these stakeholders. Shareholders, Investors

and Regulators are some of the stakeholders.

5. C. One of the key components of Corporate Governance is ensuring transparency. This promotes effective governance through establishing, communication and monitoring of performance. Employee rights are not the focus of corporate governance. Security policy as prepared by the IT as applicable for the enterprise is approved by the board. Corporate governance requirements do not provide any specific details of risk assessment but only outline need for implementing risk management as appropriate for the enterprise.

6. D. Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Risk acceptance levels are set by senior management, not by IT management. The business strategy drives the IT strategy, not the other way around. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

7. C The primary objective of Business Governance is to ensure performance and hence the focus by Board is to understand and implement key performance drivers. The other options are related to operational areas which are dealt by management at their level as required.

8. D. The Board/senior management play the most critical role in ensuring the effectiveness of the IT governance structure and processes. Hence, the effectiveness of Governance is directly dependent upon their level of involvement. The head of business units work on implementing the directions of the board and are focussed on management. The internal auditor department play an important role in evaluating how well IT governance is implemented but their role is providing guidance. The technology management is responsible for aligning IT strategy in line with the enterprise strategy and implementing IT solutions which help meet enterprise objectives.

9. B. Implementing EGIT requires active collaboration between the board/senior management in directing IT towards enterprise objectives and putting a governance framework in place. Hence, the key benefit of EGIT is the improved transparency and understanding of IT's contribution to business which is reflected in the performance management system. Although identification of relevant laws, regulations and policies requiring compliance is important in implementing EGIT, this is not the primary benefit. Directly, the focus of EGIT is neither on better utilization of human resources by using automation or on increased revenues and higher return on investments although they are considered as required.

10. A. The primary objective for implementing ERM is it helps in deciding and implementing the right level of controls. The other 3 options are indirect benefits of implementing ERM.

Chapter 2

GRC Frameworks and Risk Management Practices

Learning Objective

As IT increasingly becomes a key enabler in enterprises of all types and sizes and there is transformation of enterprises from “Technology Oriented” to “Business and Technology oriented, governance and risk management become imperative to ensure value creation and compliance. In the first chapter, we have understood how EGIT implementation can help in balancing performance with conformance. Use of best practices framework helps in balancing risk vs return by implementing the right level of security. Implementing EGIT principles is critical to strive and thrive in the highly intensive IT era. Governance frameworks provide the structure within which the management can effectively operate to deliver results as per set objectives. A governance framework typically set in in motion by the board of directors defines the rules under which the management system operates to translate the board strategy into specific actions. Governance is about ensuring that the required authority and responsibility is allocated appropriately within the organisation. It defines the boundaries of decision making together with mechanism that ensures that performance is monitored, and risks are identified and escalated so they are managed at the appropriate level. Risk management at enterprise level encompassing all levels and all areas is critical for successful implementation of governance. Governance, Risk and Compliance is a regulatory requirement, and this can be effectively implemented using well established frameworks. There are a plethora of frameworks for implementing GRC and EGIT. This chapter provides overview of some of the key GRC frameworks and also elaborates key concepts of risk management from strategy to operations.

2.1 Introduction

IT is key enabler of enterprises and forms the edifice on which the information and information systems are built. Implementing Governance, risk management and internal controls is not only a management requirement but is also mandated by law. In an IT environment embedding the right level of controls within the information systems to ensure that users can access required information securely and safely and as per business requirements is critical for survival. This not only ensures business success but is also a key requirement for the continued growth of the enterprise. In implementing internal controls in an IT environment, the legacy approach of considering IT and its contents as boxes to be secured by the IT department is fraught with extreme risk as the traditional methods of securing IT from perimeter perspective is no longer relevant. Users of I&T need to access and use information

from anywhere, anytime. There is need to adapt a macro level and architecture perspective for securing information and information systems. Hence, both from regulatory as well as enterprise perspective, senior management have to be involved in providing direction on how governance, risk and control are implemented using a holistic approach encompassing all levels from strategy to execution. The Board of directors have to evaluate, direct and monitor effective use of I&T to achieve enterprise objectives. This governance approach will ensure harnessing the power of information and information technology for achieving business objectives in addition to meeting regulatory requirements. Best practices framework provide management with distilled knowledge of experts and this can be customized to meet stakeholder requirements which include inter alia management and regulators. Management has to choose the right mix of frameworks for implementing governance, risk, security and controls. IS Auditors can assist management in implementing these frameworks in an advisory capacity or provide assurance on how well the GRC frameworks have been implemented to meet stakeholder requirements and provide recommendations for improvement. From regulatory perspective, management have to certify whether Risk management and internal controls have been implemented as per organisation needs and auditors have to certify whether this implementation is appropriate and adequate.

2.2 GRC Frameworks (including COBIT 2019, ISO 27001, ISO 31000)

2.2.1 COBIT 2019

The globally recognized COBIT 2019 Framework, the leader in ensuring effective and strategic enterprise governance of information and technology (EGIT), has been updated with new information and guidance—facilitating easier, tailored implementation. As per COBIT 2019, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. The heart of the COBIT 2019 framework incorporates an expanded definition of governance and updates COBIT 2019 principles while laying out the structure of the overall framework. The COBIT 2019 Core Model and its 40 Governance and Management objectives provide the platform for establishing your governance program; the performance management system is updated and allows the flexibility to use maturity measurements as well as capability measurements; introductions to design factors and focus areas offer additional practical guidance on flexible adoption of COBIT 2019, whether for specific projects or full implementation.

COBIT 2019 can be used as a benchmark for reviewing and implementing governance and management of enterprise I&T. COBIT 2019 is a contemporary iteration of the popular I&T governance framework and certificate. The principles and components of the governance system make COBIT 2019 an effective tool for implementing EGIT and helps enterprises in various ways such as: simplify complex issues, deliver trust and value, manage risk, reduce

potential public embarrassment, protect intellectual property and maximize opportunities. The best practices of COBIT 2019 helps enterprises to create optimal value from I&T by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

COBIT 2019 enables I&T to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and I&T functional areas of responsibility, considering the I&T related interests of internal and external stakeholders. COBIT 2019 helps enterprises to manage I&T related risk and ensures compliance, continuity, security and privacy. COBIT 2019 enables clear policy development and good practice for I&T management including increased business user satisfaction. The key advantage in using a generic framework such as COBIT 2019 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

2.1.1.1 Integrating COBIT 2019 with Other Frameworks

There is no single framework which provides all the requirements for all types of enterprises. Hence, enterprises have to select the right blend of frameworks and best practices. The main advantage of using COBIT 2019 is that it is provides an enterprise view and is aligned with enterprise governance best practices enabling EGIT to be implemented as an integral part of wider enterprise governance. COBIT 2019 also provides a basis to integrate effectively other frameworks, standards and practices used such as ITIL, TOGAF and ISO 27001. It is also aligned with The EGIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of I&T, covering responsibility, strategy, acquisition, performance, compliance and human behaviour that the governing body (e.g., board) should evaluate, direct and monitor. Thus, COBIT 2019 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language.

The Governance and Management objectives in Cobit 2019 are grouped in to five Domains. Governance objectives are grouped in the Evaluate, Direct and Monitor (EDM) Domain. In this Domain the Governing body Evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy. Management Objectives are grouped into four Domains:

Align Plan and Organise (APO) addresses the overall organization strategy and supporting activities for I&T.

Build, Acquire and Implement (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.

Deliver, Service and Support (DSS) addresses the operational delivery and support of I&T Services

Monitor, Evaluate and Assess (MEA) addresses performance monitoring and conformance of I &T with internal performance targets, internal control objectives and external requirements.

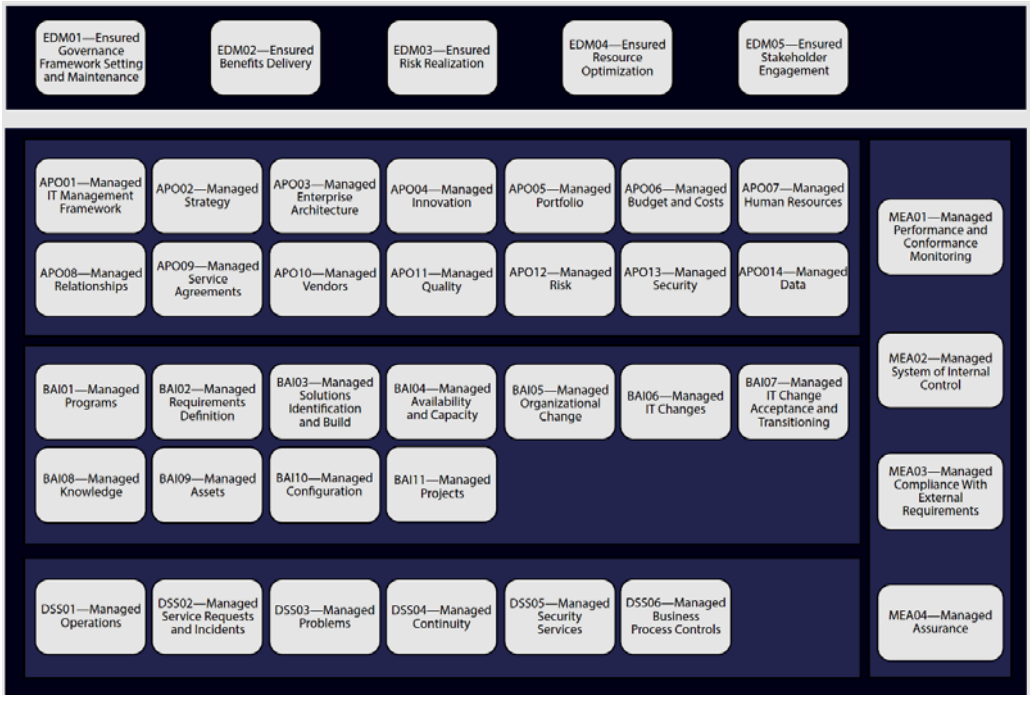

Figure 2.1: CO*BIT 2019 40 governance & management objectives*

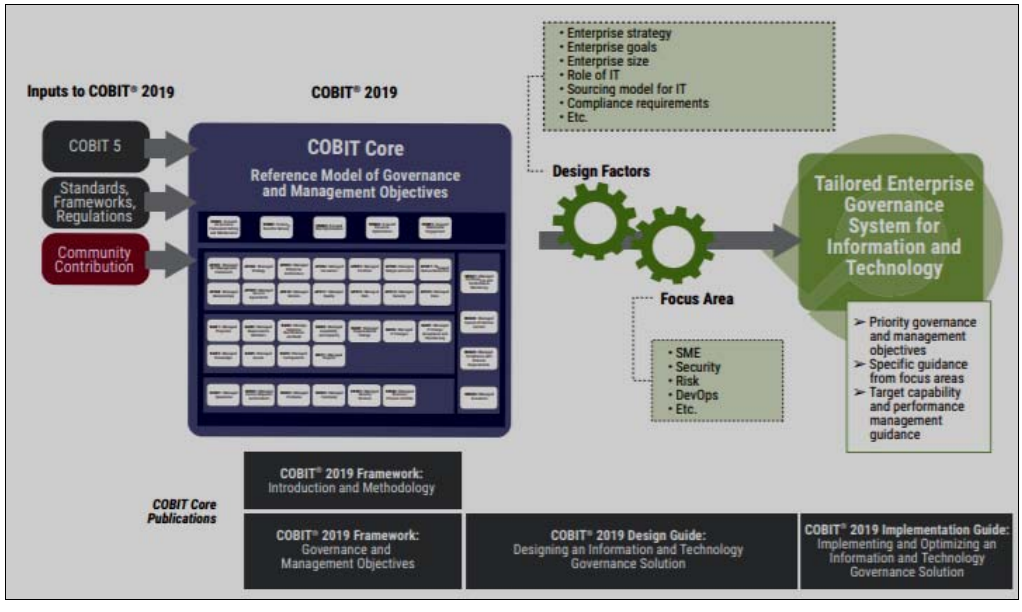

Figure 2.2: COBIT 2019 Overview

2.2.2 ISO 27001

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyses and addresses its information security risks. The ISMS ensure that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach. The Standard is designed to help organizations manage their information security processes in line with international best practice while optimizing costs. It is technology and vendor neutral and is applicable to all organizations - irrespective of their size, type or nature.

A part of the ISO 27000 family of standards, ISO 27001 consists of 114 controls and 10 management system clauses that together support the implementation and maintenance of the standard.

ISO 27001 emphasizes the importance of risk management, which forms the cornerstone of an ISMS. All ISO 27001 projects evolve around an information security risk assessment - a formal, top management-driven process which provides the basis for a set of controls that help to manage information security risks.

ISO/IEC 27001 is a formalized specification for an Information System Management System (ISMS) with two distinct purposes:

1. It lays out, at a high level, what an organization can do in order to implement an ISMS
2. It can (optionally) be used as the basis for formal compliance assessment by accredited certification IS Auditors in order to certify an organization.

By implementing an ISO 27001-compliant ISMS, organisations will be able to secure information in all its forms, increase their resilience to cyber-attacks, adapt to evolving security threats and reduce the costs associated with information security.

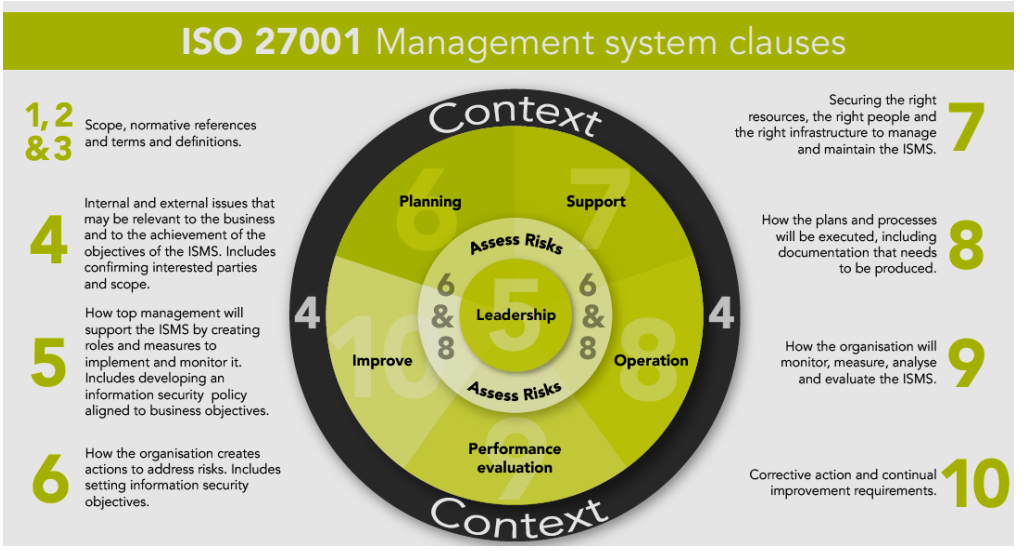

Figure 2.3: ISO 27001 Management System Clauses

2.2.2.1 ISO/IEC 27001: 2013 controls

1. A.5 Information security policies
2. A.6 Organisation of information security
3. A.7 Human resources security
4. A.8 Asset management
5. A.9 Access control
6. A.10 Cryptography
7. A.11 Physical and environmental security
8. A.12 Operational security
9. A.13 Communications security
10. A.14 System acquisition, development and maintenance
11. A.15 Supplier relationships
12. A.16 Information security incident management
13. A.17 Information security aspects of business continuity management
14. A.18 Compliance

2.2.3 ISO 31000

ISO has developed a new standard for IT risk management. The standard primarily adopts

AS/NZS 4360 for risk management. The modification it has made is that ISO has added processes for IT risk governance by defining IT risk committee. ISO 31000:2018, Risk management – Guidelines, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector.

Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance.

2.2.4 ISO 38500:2015

ISO/IEC 38500 is an international standard for Corporate governance of information technology published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations' use of IT.

ISO/IEC 38500:2015 provides guiding principles for members of governing bodies of organizations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organizations.

It also provides guidance to those advising, informing, or assisting governing bodies. They include the following:

- executive managers;
- members of groups monitoring the resources within the organization;
- external business or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies;
- internal and external service providers (including consultants);
- auditors.

ISO/IEC 38500:2015 applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization. ISO/IEC 38500:2015 defines the governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance.

ISO/IEC 38500:2015 is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations. ISO/IEC 38500:2015 is applicable to organizations of all sizes from the smallest to the largest, regardless of the extent of their use of IT.

The purpose of ISO/IEC 38500:20015 is to promote effective, efficient, and acceptable use of IT in all organizations by

- assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have confidence in the organization's governance of IT,
- informing and guiding governing bodies in governing the use of IT in their organization, and
- establishing a vocabulary for the governance of IT.

2.3 Enterprise Risk Management

2.3.1 Risk Management

Enterprise Risk Management and I&T Risk Management are key components of an effective I&T governance structure of any enterprise. Effective I&T governance helps to ensure close linkage to the enterprise risk management activities, including Enterprise Risk Management (ERM) and I&T Risk Management. I&T governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite. The risk assessment approach adapted has to consider business impact of IS risk and different types of risks. There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the I&T risk profile. This section will provide an overview of related terms like threats, vulnerabilities etc., IS Risks and exposures and risk mitigation strategies, which can be adapted by the organizations.

Risk management process is a crux of any business today and it is a day-to-day activity. Risk management processes primarily focuses on three major areas viz. Market Risk, Credit risk and Operational Risk. Most organization addresses first two risks i.e. market risk and credit risks since these are part and parcel of business activities. Whereas operational risks address the issues and concerns related to operations of a business. Today's organizations depend heavily on information and related technology and majority operations have been automated. Hence, it is important to consider IT risks as these by themselves are very critical but in terms of impact on other risks, they can impact all areas of enterprise operations. Hence, it is important to understand how the use of technology has introduced various new types of risks and their impact specifically in organizations which are heavily dependent on technology. The Figure below describes the relationship on technology risks in overall risk scenario.

Figure 2.4: Relation of IT risks

2.3.2 Risk Management in COBIT 2019

I&T Risks have to be managed from holistic perspective and this approach is called risk optimisation. The COBIT 2019 framework provides excellent guidance on risk management strategy and practices from governance and management perspective. COBIT 2019 aims to continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. The Governance Domain contains five Governance processes and one of the Governance process EDM03: Ensured Risk Optimisation primarily focusses on stakeholders' risk-related objectives. The objective of this process is to ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated and that risk of I&T is identified and managed. The key benefits of implementing appropriate risk optimisation process is that it ensures that I&T-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures are minimised. The Cobit framework 2019 has management domain of Align, Plan and Organise which contains a risk related process APO 12: Managed Risk. This process requires continually identifying, assessing and reducing I&T related risk within levels of tolerance set by enterprise executive management. The primary purpose of this process is to integrate the management of I&T related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T related enterprise risk.

Key Governance Practices of Risk Management (EDM 03: Ensured Risk Optimisation)

Implementing governance requires that governance practices covering all the aspects of governance of risk management are covered. There are three broad areas:

- Evaluate Risk Management: Continually examine and make judgment on the effect of risk on the current and future use of I&T in the enterprise. Consider whether the

enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T are identified and managed;

- Direct Risk Management: Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate to ensure that the actual I&T risk does not exceed the board's risk appetite; and
- Monitor Risk Management: Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

Key Management Practices of Risk Management (APO 12: Managed Risk)

Implementing Risk Management requires that the risk management practices are embedded in all the key organisational processes as required and are performed as part of the day to day tasks and activities. A process-oriented approach has to be followed for implementing risk management. The key management practices of effective risk management are:

- Collect Data: Identify and collect relevant data to enable effective I&T related risk identification, analysis and reporting.
- Analyze Risk: Develop a substantiated view on actual I&T risk in support of risk decisions.
- Maintain a Risk Profile: Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
- Articulate Risk: Provide information on the current state of I&T- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- Define a Risk Management Action Portfolio: Manage opportunities and reduce risk to an acceptable level as a portfolio.
- Respond to Risk: Respond in a timely manner with effective measures to limit the magnitude of loss.

Metrics of Risk Management

Enterprises have to monitor the processes and practices of I&T risk management by using specific metrics. Some of the key metrics are:

- Percentage of critical business processes, I&T services and I&T-enabled business programs covered by risk assessment;
- Number of significant I&T related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including I&T related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

2.3.3 Risk Factors

There are unique risks for each organization, given the nature of operations, although generally organizations within the same sector will have common risk elements. The appropriate risk response will be different from organization to organization, depending on how management views the risk in terms of magnitude. Risks are represented in the external environment in which the organization chooses to operate, as well as those in the internal environment. Risk factors in the external environment are generally outside of the organization's direct control. External risk factors include political situations, the economy, regulations, natural disasters, competition. Internal risk factors include Organization's culture, Internal environment affecting employee's moral, policies, ethics and values projected by senior management, process environment, control environment and so on.

2.3.4 Categories of Risks

The risk management process begins with the identification of risk categories. An organization will have several risk categories to analyse and identify risks that are specific to the organization. Some examples of risk categories are:

- Business Risks: Also, sometimes referred as inherent risks. These are risk associated with nature of business. E.g. loss of finished product for food industry
- Market Risks: Risks associated with fluctuations on market affecting the customer base of organization. E.g. Customer preferring smart phones over traditional phones affecting Nokia products.
- Financial Risks: Risk associated with financial decisions and environment in which business operates. E.g. Non-availability of funds, excess expenditure etc.
- Operational Risks: Risks associated with failure of operations of organization. E.g. failure of assembly-line for car manufacturer, non-availability of IT for banking services etc.
- Strategic Risks: Associated with incorrect and inappropriate strategy selection and implementation. E.g. Planning for implementing IT application that is outdated, selecting application for automation that may not satisfy future growth expectations. Not-considering effect of smart phones by Nokia management.
- IT Risks: How the company's IT infrastructure relates to business operations and their impact on business in case risk materializes. E.g. failure of networks affecting communications, failure of applications impacting operations and service delivery.
- Compliance Risks: Risk when an organization does not comply with legal, regulatory, contractual or internal compliance requirements E.g. failure of complying with privacy laws, labour laws, software license agreement.
- Reputational Risk: Reputational risk is the chance of losses due to a declining

reputation as a result of practices or incidents that are perceived as dishonest, disrespectful or incompetent.

E.g. loss of sales and increased costs such as fines or legal fees.

- Process Risk: The business risk associated with a particular process. Process tend to be a focus of risk management as reducing risk in core business process can often yield cost reductions and improved revenue. Risk related to P2p cycle or O2c cycle.

2.3.5 Elements of Risk Management

Before establishing a strategy for information risk management, the following elements must be in place to permit effective risk management:

- Top Management Support: The need for risk management must start and be supported at the highest level within the company. This includes the governance level and the CEO.
- Proactive Approach: Risk management efforts must be proactive. This involves the active identification, measurement and management of the risks, scanning of changes in the risk profile and reports on managing the risk profile.
- No Ambiguity: There needs to be a clear definition of the risks, and these must be understood across the organization.
- Accountability: Responsibility for responding to and managing the risks must be clearly understood and individuals held accountable for fulfilling the roles.
- Resource Allocation: Appropriate resources including people and tools need to be deployed and available to help managers, executive and the governance level conduct their obligations within the risk management framework.
- Cultural Change: The organization's culture must provide for the active management of risk.

2.3.6 Developing Strategies for Information Risk Management

Some organisations have adopted a centralized model for risk management, while others are using a decentralized model. The approach depends on:

(a) An organization's particular operations,

(b) The significant risks,

(c) The culture of the organization,

(d) The management style and

(e) The control environment i.e. the degree of centralization or the delegation of authority and the infrastructure of the business.

In a centralized model it is the Information Risk Management team that develops policies for the board to consider. Other organizations have decentralized model requiring the involvement of front-line staff in managing the inherent risks of the company, of the business unit or of the process.

2.4 Risk Management Process

The Objective of risk management process is to ensure that the organization can manage risks within acceptable limits. These acceptable limits are decided by Risk Appetite ad Risk tolerance.

Risk Appetite: It is ability of organization to sustain losses due to materialization of risk. It also represents the ability of organization to take risk while considering new business initiatives. It can be defined as 'the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives.

Risk Tolerance: It is the limit up to which organization can tolerate to sustain loss of business in case risk materializes. In other words, in case any risk materializes the organization must recover from it within specified time decided by risk materialization.

Information Risk Management process involves a continuous cycle to identify, assess, measure, decide response, assign responsibility and monitor information risk. Organization may adopt any standard or framework discussed earlier for implementing Information risk management. Although different framework describes different processes for managing IT risks, typically IT risk management process follows following steps:

1. Establish the Context
2. Risk identification
3. Risk evaluation
4. Risk prioritization
5. Risk response
6. Risk mitigation
7. Risk monitoring

2.4.1 Risk Identification

As name suggest it is processing to identify risks for organization. Organization may deploy one or more methods to identify risks. Some methods are:

1. Workshop and brainstorming sessions with stakeholders and process owners: In this method the process owners and risk practitioners (IS Auditors) meet and discuss the possible causes for process failures affecting desired outcome. This workshops typically

covers risk identification, risk evaluation, control definition steps. In case process owners does not agree a method called Delphi technique be used to assess the risks.

2. Use of generic risk scenarios based on industry experience and historical data: Generic scenarios are the list of possible incidents affecting desired outcome of business process objectives.

3. Review and audit of processes and technology. This includes vulnerability assessment: Audit findings, lessons learned from Incident response, vulnerability assessments help organization in identifying possible threats that can impact the normal functioning of business processes.

2.4.1.1 Risk Components

Risk to be managed effectively have to be understood in totality. Hence, it is important to understand all the specific components of all identified risks and these are:

- Risk Scenario: A possible event due to materializing of one or more risks for example Failure of connectivity might be caused due to one or more reasons like physical damage to cables / devices, malfunction of devices, virus / malware attack, Denial of service attack, failure of service provider.
- Threat: Reason for risk materialization for example theft of equipment, fire, natural disaster, non-availability of human resources, Virus
- Vulnerability: Weakness that gets exploited due to threat. For example, absence of antivirus is a vulnerability that will enable a virus to infect the system or improper physical security leading to theft
- Likelihood / Probability: Judgment of possibility that threat shall exploit vulnerability. For example, there is always a possibility of earthquake, however it may not take place every day. The possibility can be worked out based on historical data and seismic zone in which facility is located. Or possibility of virus attacking systems can happen multiple times in a day.
- Impact / Consequences: When threat materializes, it will affect normal functioning which might result in loss of business, interruption of services. A calculation of possible loss expressed in monetary terms.
- Response: Acton Plan designed by organization to minimize impact or likelihood of risk materializing. There are four types of responses and organization may choose one or more for each risk. The four types are: Accept, Transfer, Avoid and Mitigate. For example, Management may have process to monitor virus by maintaining antivirus tool updated and also run a schedule scan. In case cost of process and tool is higher than impact organization may decide to do nothing and accept the risk.
- Controls / Mitigation: In order to mitigate risk management implements controls. For

example, Access controls reduces the likelihood of unauthorized access, Fire suppression system reduces the impact due to fire.

- Inherent Risk: Total risk without any controls is inherent risk.
- Residual Risk: Controls cannot mitigate the risk completely. It may reduce likelihood and/or impact. There is a small portion of risk still remains that is known as residual risk. It also includes accepted risk.
- Risk Aggregation: A risk faced by organization may have different impact on different business function/ locations. However, from organization's perspective it is necessary to present them as total risk for organization. For example, a location on sea shore may have higher risk of flooding as compared to another location away from seashore.
- Risk Profile: Collective view of all risks an organization likely to face.
- Heat Map: Graphical representation of risk profile.
- Risk Register: A document that is maintained to provide information on identified risks and contents details of components.
- Risk Owner: Person or entity that is responsible for evaluation and decision of response for identified risk.

Organizations may adopt various methods for identifying and recording risks some of them are discussed here.

2.4.1.2 Threat Profile / Inventory

It is a list of all possible threats that might have impact on organization. Organization may prefer to categorize them based on nature.

- Physical and Environmental for example fire, theft, humidity, temperature
- External threats that are not in control of organization like hackers, Denial of service, virus, sabotage, targeted attacks
- Internal threats are those are initiated within organization for example disgruntled employee, unauthorized access by authorised users, confidential data leakage by employee, misuse of management override. Majority breaches are due to internal threats
- Natural threats like earthquake, floods, and tsunami

Organization may prepare a list of threats and try to evaluate how they affect organization.

2.4.1.3 Vulnerability Assessment

A vulnerability assessment is one of the process of identifying, the vulnerabilities in a system. Vulnerability assessment is one process in risk identification. The Vulnerability Assessment is an evaluation to identify gaps and vulnerabilities in your network, servers, etc. help you validate your configuration and patch management, and identify steps you can take to improve

your information security. The assessment helps you meet your minimum compliance mandates and security assessment needs. Assessments are typically performed according to the following steps:

a. Cataloguing assets and resources in a system.

b. Assigning quantifiable value or rank and importance to those resources

c. Identifying the vulnerabilities or potential threats to each resource

Vulnerabilities that may exist across your systems and applications can create an easy path for hackers to gain access to and exploit your environment. With dozens and even hundreds of applications and systems across your environment with access to the Internet, maintaining and updating system operating systems and applications to eliminate vulnerabilities is paramount - especially when those applications and systems are tied to sensitive customer, patient or cardholder information.

2.4.1.4 Asset Inventory

Risks when materialize affect the functioning of organization. The impact of a risk can be different for different business function depending upon the various factors like time of incident, functions affected etc. For example, in case on a Bank failure of connectivity might affect ATM network as well as branch network, however if the failure happens after business hours impact of non-availability of ATM could be higher. In other words, providing protection for connectivity to ATM shall be different as compared to branch networks. In order to provide appropriate security organizations may focus on implementing controls over assets that supports business processes. ISO27001:2005 also recommends implementing controls around assets by prioritizing them based on results of risk evaluation. (ISO27001:2013 recommend ISO31000 for Risk management and also states that risk management need not be asset based.)

2.4.1.5 Risk Register and Control Catalogue

It is a collective record of all identified and evaluated risk along with risk owner and risk response. The structure of risk register may vary organization to organization, however it must:

1. Contain risk scenario, likelihood, assets impacted, overall impact on business (assessment), owner, risk response decision, reference to control catalogue, review date.

2. It must be maintained based on updating process.

3. Generally, it is used to develop risk profile for reporting to management and approval.

IS auditor should use this risk register to review and audit the risk management process and also ensure that appropriate controls are identified, designed and implemented. Control catalogue is collective register of all controls designed and implemented within organization with reference to risk register.

2.4.2 Risk Evaluation

Also called risk assessment. It is a process for assessing likelihood and impact of identified risk. There are two methods used for risk evaluation

1. Quantitative Risk Analysis refers to expressing total risk in monetary terms
2. Qualitative Risk Analysis refers to expressing total risk with qualification like high, medium, low etc. However, the challenge is perception of these terms differs from person to person, hence it is necessary to define the meaning of terms high, medium and low so that they are interpreted uniformly across organization.

2.4.3 Determine Likelihood of Risk

Once threats are identified, the next step is to determine the likelihood that the potential vulnerability can be exploited by those threats. Several factors need to be considered when determining this likelihood.

(a) Consider source of the threat, motivation behind the threat, and capability of the source.

(b) Determine the nature of the vulnerability and,

(c) The existence and effectiveness of current controls to deter or mitigate the vulnerability. The likelihood that a potential vulnerability could be exploited can be described as high, medium, or low.

Most of the time the likelihood is judgment of analysts hence it is best estimated by risk owners who are the business process owners as they are likely to be affected due to risk materialization. This helps in arriving at likelihood.

2.4.4 Risk Prioritization

Based on evaluation of risks, the risks have to be prioritised into high, medium or low or ranked on scale of 1 to 5. This risk ranking will help enterprises to decide the priority in which the risks will be mitigated. Based on the decisions taken in this process/stage, the next step of risk response is implemented. The organizations generally use Risk profile and Heat map to prioritize evaluated risks based on criticality of risks and priorities of business objectives.

Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophe 5
Almost Certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

Figure 2.5: Risk optimisation

2.4.5 Risk Response

With the potential impact assessment in hand, the next step is to determine what the appropriate response is to prudently manage the risk.

When risks are identified and analysed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is illustrated below:

Figure 2.6: Risk Response

The risk mitigation strategy is explained for each of the options.

- Accept the Risk. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- Avoid the Risk. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be avoided/ eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- Transfer the Risk. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
- Mitigate the Risk. Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.

For each risk identified, the risk response can be articulated the objective is to bring the estimated risk below the Risk appetite and risk tolerance of the organization. For example, where the risk response is to accept the risk, this becomes part of the organization's risk tolerance, means the business must recover from impact before tolerance limits.

Figure 2.7: Relationship of Risks and Controls

2.4.6 Risk Monitoring

Once the controls are implemented what remains is residual risk i.e. risk remaining after implementing controls and risk accepted. For example, Organization may implement fire resistant material to reduce the likelihood of risk. They also implement policies regarding use of inflammable material and safe electrical design using circuit breakers. Still if the fire breaks out smoke detectors are implemented to get early warning so that the incident can be responded to contain damage. Depending upon the level of impact organization may install fire suppression system that will be automatically activated based on temperature levels and response time and hence damage is further reduced. However there still remains risk of fire and hence it needs to be monitored by including processes for testing control equipment, processes etc. Risk monitoring is process consists of following activities:

1. Periodic review identified and evaluated risks to confirm that the evaluation is appropriate. This might change due to various factors like changes in environment, business strategy and focus, Market changes and so on.
2. Review of risks associated with changes in infrastructure, processes and IT. Change might have effect on risks, for example organization has implemented uninterruptible power supply system. Subsequently it might have added more equipment and hence the capacity of UPS may not be sufficient in future. Identifying evaluating this risk in time shall reduce impact of failure.
3. Incident response and lessons learned is another area that prompts for review of risks that materialized.
4. Audit findings also requires review of risks since non-effective controls might provide false comfort of compliance to management.

2.5 IS Risks and Risk Management

There are numerous changes in IT and its operating environment that emphasizes the need to better manage IT related risks. Dependency on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. Increasing disclosures of information system disasters and increasing electronic fraud, in turn, drive this. The management of IT related risks is now being understood as a key part of enterprise governance.

Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. This security has to be implemented as per required control system envisaged by the management of the enterprise. The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in

computer systems is restricted to authorized people".

IS Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them.

2.6 Compliance in Cobit 2019

The Management Domain of ”Monitor, Evaluate and Assess” has a compliance focused process namely:MEA03:Managed Compliance with External Requirements”. This process is designed to Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. This requires that the enterprise has process in place to obtain assurance that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance. The primary purpose of this process is that the enterprise is compliant with all applicable external requirements.

2.6.1 Key Management Practices of IT Compliance

COBIT 2019 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. These practices can be adapted as required:

- Identify External Compliance Requirements: On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an I&T perspective.
- Optimize Response to External Requirements: Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and good practice guidance for adoption and adaptation
- Confirm External Compliance: Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements
- Obtain Assurance of External Compliance: Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

2.6.2 Key Metrics for Assessing Compliance Process

Implementing compliance practices requires monitoring of metrics. A list of sample metrics for reviewing the process of evaluating and assessing compliance are given here for both areas of compliance with external laws and regulations and IT compliances with internal policies:

2.6.2.1 Compliance with External Laws and Regulations:

- Cost of IT non-compliance, including settlements and fines;
- No. of IT related non-compliance issues reported to board or causing public comment or embarrassment;
- No. of non-compliance issues relating to contractual agreements with IT service providers;
- Coverage of compliance assessments.

2.6.2.2 IT Compliance with Internal Policies:

- Number of incidents related to non-compliance to policy;
- Percentage of stakeholders who understand policies;
- Percentage of policies supported by effective standards and working practices; and
- Frequency of policies review and updates.

2.7. Information Technology Act 2000

The Information Technology Act 2000, (Amended 2008) provides that any organization is collecting PII shall be liable in case absence of reasonable security of such information results in identify theft. It introduced new provisions which are specifically applicable to corporates, provisions relating to maintaining privacy of information and imposed compliance requirements on management with penalties for non-compliance. These requirements have to be considered as part of compliance by corporates and individuals as applicable.

The specific areas of compliance which could be reviewed by the IS Auditor are:

Section 43 A

- Are various components of "sensitive personal data or information" vis-à-vis users/customers defined by the enterprise?
- Does the enterprise have a security policy?
- Is the security policy documented?

Section 69B

- Has the enterprise adopted/established appropriate policy, procedures and safeguards for monitoring and collecting traffic data or information?
- Are these documented?

Section 70B

- Does the enterprise have appropriate documented procedure to comply with the requests of CERT-IN regarding cyber security incidents?

Section 72A

- Does the enterprise have an adequate privacy policy?
- Whether the enterprise has provided for opt-in/opt-out clause in the privacy policy?

General

- Has the enterprise appointed designated officer/nodal officer/computer-in-charge to comply with the directions of competent authority/agency under various provisions of the Act? Whether details of such designated officer/nodal officer readily available online (at its website)?

Section 7A Audit of documents i.e. in Electronic Form: Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information, processed and maintained in electronic form.

Under Section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

The IT Act 2008 recognizes and punishes offences by companies and individual (employee) actions. For example: Section 66 to 66F and 67 deal with the following crimes:

- Sending offensive messages using electronic medium or using body corporate's IT for unacceptable purposes
- Dishonestly stolen computer resource
- Unauthorized Access to computer resources
- Identity theft/Cheating by personating using computer
- Violation of privacy
- Cyber terrorism/Offences using computer
- Publishing or transmitting obscene material

Under Section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years or fine extending to INR 5,00,000 or with both.

2.8 General Data Protection Regulation (GDPR)

The introduction of European Union's ("EU") regulations on protection of natural persons with regard to processing of personal data and free movement of such data GDPR has brought on certain significant implications on Indian entities processing personal data of EU Residents. Basically, since GDPR has extra-territorial application and applies to processing of personal data of EU residents even by entities situated outside EU, Indian entities who are acting as either a 'controller' (i.e. the person who determines the purposes and means of the processing of data) or a 'processor' (i.e. the person who processes the personal data on behalf of the controller), of personal data of persons of EU, in relation to offering of goods or services to such persons or monitoring their behaviour in so far as it takes place within EU, become subject to GDPR.

The concept of "personal data" has been defined in GDPR to refer to any information relating to an identified or identifiable natural person (i.e. "Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, and therefore all such information is considered as 'personal data' under the GDPR.

For Indian companies dealing with such 'personal data' of EU residents, it then becomes imperative to implement the data protection requirements stipulated in GDPR within their systems. This requires a significant overhaul and re-writing of their privacy policies and contractual arrangements with EU counterparts/Data Subjects and their internal data protection protocols and systems to make them GDPR compliant.

Compliance with GDPR has become particularly important given the heavy penalties associated with GDPR non-compliance. Failure to comply with the GDPR requirements can attract administrative fines of up to EUR 10,00,000 or 20,000,000, or in the case of an undertaking, up to 2% or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, depending on the nature of provisions breached. Also, for Indian Company with business dealings with EU companies, their EU counterparts are also likely to insist on compliance with the GDPR as part of their standard contractual clauses. We may also add that the Indian Government is also seeking to introduce a more robust regulatory framework for data protection and privacy. Therefore, companies having business interest in EU should take comprehensive look at evolving their data protection practices not just to be GDPR compliant but also in preparation for a more stringer data protection regulatory framework likely to be introduced in India in the near future.

2.9 The Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019 seeks to provide for protection of personal data of

individuals, and establishes a Data Protection Authority for the same.

The Bill governs the processing of personal data by:

(i) government,

(ii) companies incorporated in India, and

(iii) foreign companies dealing with personal data of individuals in India.

Personal data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government.

Obligations of data fiduciary: A data fiduciary is an entity or individual who decides the means and purpose of processing personal data. Such processing will be subject to certain purpose, collection and storage limitations. All data fiduciaries must undertake certain transparency and accountability measures such as:

(i) implementing security safeguards (such as data encryption and preventing misuse of data), and

(ii) instituting grievance redressal mechanisms to address complaints of individuals.

Rights of the individual: The Bill sets out certain rights of the individual (or data principal). These include the right to:

(i) obtain confirmation from the fiduciary on whether their personal data has been processed,

(ii) seek correction of inaccurate, incomplete, or out-of-date personal data,

(iii) have personal data transferred to any other data fiduciary in certain circumstances, and

(iv) restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

Transfer of data outside India: Sensitive personal data may be transferred outside India for processing if explicitly consented to by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as critical personal data by the government can only be processed in India.

Offences: Offences under the Bill include:

(i) processing or transferring personal data in violation of the Bill, punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher, and

(ii) failure to conduct a data audit, punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher.

(iii) Re-identification and processing of de-identified personal data without consent is

punishable with imprisonment of up to three years, or fine, or both.

2.10 Summary

This chapter has provided an overview of various types of Governance and risk management frameworks which can be used by organisations for implementing. There is no single framework which meets all requirements. Hence, it is important to understand the scope and coverage of each of these frameworks so that they can adapted as required for implementation. Risk management is an integral aspect of governance and management. Risks have both positive and negative attributes. Risks provide challenges but they also provide opportunities. Risk management requires effective mitigation of risks by adapting the risk management process strategy thereby balancing risk versus benefits.

2.11 Questions

1. The most important requirement for IT governance function to be effective is:
   A. Monitoring
   B. Evaluation
   C. Directing
   D. Managing
2. The MOST important benefit of implementing IT risk management process is that it helps in:
   A. optimizing internal control framework.
   B. ensuring residual risk is at acceptable level.
   C. prioritizing business functions for audit planning.
   D. complying with regulatory requirements.
3. Which of the following is a major risk factor?
   A. Existence of inflationary trends.
   B. Vendor launches new software.
   C. Board of directors elects new chairman.
   D. Change in government post elections.
4. The level to which an enterprise can accept financial loss from a new initiative is:
   A. Risk tolerance
   B. Risk management
   C. Risk appetite
   D. Risk acceptance

5. Designing and implementing a control to reduce the likelihood and/or impact of risk materializing is a:
   A. Risk acceptance
   B. Risk transfer
   C. Risk treatment
   D. Risk transfer
6. Which of the following is a valid risk statement?
   A. Network service provider is unable to meet bandwidth.
   B. Hacker attempts to launch attack on web site.
   C. Application server crash due to power failure.
   D. Delay in servicing customers due to network congestion.
7. Which of the following is primary reason for periodic review of risk? The changes in:
   A. risk factors
   B. risk appetite
   C. budget
   D. risk strategy
8. Which of the following is a strategic IT risk?
   A. IS audit may not identify critical non-compliance.
   B. Non-availability of networks impacting services to customers.
   C. New application may not achieve expected benefits.
   D. Defer replacement of obsolete hardware.
9. Which of the following is the most essential action after evaluation of inherent risks?
   A. Evaluate implemented controls.
   B. Update risk register.
   C. Prepare heat map.
   D. Prioritized evaluated risk.

2.12 Answers and Explanations

1. C. Directing is the most critical of the Governance function which can be performed by the Board. Although, governance has three critical functions: Evaluate, direct and monitor, evaluation and monitoring can be performed against directions.

2. B. The primary function of IT risk management process is to support value creation by reducing the risk to an acceptable level. The other options are secondary benefits of IT

risk management.

3. D. Risk factors are conditions that affect the risk profile of organization. Change in government is one of major risk factor as compared with other options.
4. C. Risk appetite denotes the level of risk acceptable by management. Risk tolerance is the time up to which an organization can afford to accept the risk. Risk management is a process of risk mitigation and risk acceptance is decision of the management and is considered as risk response.
5. C. Implementing control is a risk treatment.
6. D. Options A, B and C are threats and not risks.
7. A. Changes in risk factors is the primary reason for reviewing changes in risk levels for an organization. The other options are secondary reasons.
8. D. Deferring replacement of obsolete hardware is strategic decision and hence it is a strategic IT risk. Others are operational IT risks.
9. A. Once risks are evaluated it is necessary to find out the current state of risk mitigation (gaps in controls) by evaluating the existing controls. This help in identifying gaps and implementing controls so as to reduce the total exposure within acceptable limits. Other activities are required but not as essential as identifying gaps in controls.

Downloads

COBIT 2019 Design Guide

http://www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx

Chapter 3

Key Components of A Governance System

Learning Objectives

To satisfy governance and management objectives, each enterprise needs to establish, tailor and sustain a governance system built from a number of components. Components are factors that, individually and collectively, contribute to the good operations of the enterprise's governance system over I&T. Components interact with each other, resulting in a holistic governance system for I&T. Components of a governance system include organizational structures; policies and procedures; information items; culture and behavior; skills and competencies; and services, infrastructure and applications

COBIT 2019 which is based on components can be used for implementing Enterprise Governance of Information Technology (EGIT). This chapter discusses the key components of EGIT which facilitate the successful achievement of enterprise goals and IT enabled goals.

3.1 Introduction

Organizations which wish to implement EGIT for achieving enterprise objectives have to consider various key aspects such as goals, objectives, benefit and value for the organisation. However, to ensure these are achieved, an appropriate EGIT framework must be implemented. Implementing EGIT does not occur in a vacuum but has to consider the specific environment applicable to the enterprise. We have discussed in earlier chapters how implementation of EGIT can be focussed both on conformance and performance. EGIT implementation has to be taken as a project with an empowered project champion vested with responsibility for results. Selecting and implementing the right type of components as required is the key to successful implementation of a EGIT framework. This implementation takes place in different conditions and circumstances determined by numerous factors impacting both internal and external environment and these could be pertaining to:

- Ethics and culture of the organisation
- Laws, regulations and policies
- Applicable standards
- Industry practices
- Competitive environment

Implementing EGIT requires consideration of specific aspects applicable to the enterprise and these could pertain to:

- Mission, vision, goals and values

- Governance policies and practices
- Culture and management style
- Models for roles and responsibilities
- Business plans and strategic intentions
- Operating model and level of maturity

3.2 COBIT 2019 Governance System Principles

COBIT 2019 simplifies governance challenges with just 6 principles. The six key principles for governance and management of enterprise IT in COBIT 2019 taken together enable the organisation to build an effective governance and management framework that optimizes information and technology investments use for the benefit of stakeholders.

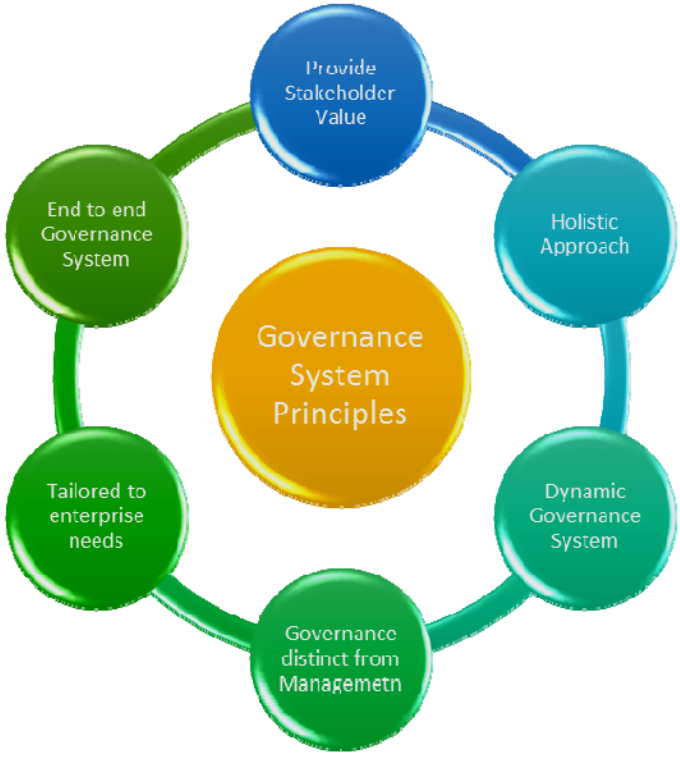

Figure 3.1: Governance Framework Principles under COBIT 2019

Principles 1: Provide Stakeholder Value: enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 2019 provides all of the required processes and other components to support business value creation through the use of I&T. Because every

enterprise has different objectives, and enterprise can customize COBIT 2019 to suit its own context through the goals cascade, translating high level enterprise goals into manageable specific, IT related goals and mapping these to specific processes and practices.

Principle 2: End-to-End Governance System: COBIT 2019 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 2019 does not focus only on the IT function but treats information and related technologies as assets that needs to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management components to be enterprise wide and end to end i.e. inclusive of everything and everyone internal and external that is relevant to governance and management of enterprise information and related IT.

Principle 3: Tailored to Enterprise Needs: A governance system should be tailored to the enterprise's needs, using a set of design factors as parameters to customize and prioritize the governance system components.

Principle 4: Holistic Approach: Efficient and effective Enterprise governance of I&T require a holistic approach, taking into account several integrating components. COBIT 2019 defines a set of components to support the implementation of a comprehensive Enterprise governance system for I&T. Components are broadly defined as anything that can help to achieve objectives of the enterprise.

Principle 5: Governance Distinct from Management: The COBIT 2019 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities require different organizational structures and serve different purposes.

- Governance: It ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed on enterprise objectives to be achieved; setting direction through prioritization and decision making, and monitoring performance and compliance against agreed on direction and objectives. In most organizations the governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities many be delegated to special organizational structures at an appropriate level, especially in larger, complex organizations.
- Management: It plans, builds, runs and monitors activities in alignment with the direction set by the governing body to achieve the objectives. In most of the enterprises; management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

Table 3.1: Distinction between Governance and Management

Governance	Management
• Evaluate: Stakeholder needs, conditions and options	• Plan, build, run and monitor activities

• Determine: Agreed on enterprise objectives	• Align with: direction set by the governance body
• Set direction: Prioritization and decision making	• Achieve: Enterprise objectives
• Monitor: Performance and compliance	• Monitor and Report: Performance and conformance
• Responsibility: Board of directors	• Responsibility: Management at all levels

Principle 6: Dynamic Governance System: A governance system should be dynamic. This means that each time one or more of the design factors are changed (e.g., a change in strategy or technology), the impact of these changes on the EGIT system must be considered. A dynamic view of EGIT will lead toward a viable and future-proof EGIT system.

3.3 Components of the Governance System as per COBIT 2019

Components are broadly defined as anything that can help to achieve the objectives of the enterprise. They are also the factors that, individually and collectively, influence whether something will work. There are seven components of COBIT 2019.We will discuss the key characteristics of each of these seven components.

Figure 3.2: Components of a Governance System

3.3.1 Principles, Policies, Procedures

The first component of COBIT 2019 is: "Principles, Policies and Procedures". It may be noted that these components although provided in COBIT 2019 from a EGIT perspective can be equally applicable and adaptable for any new project or initiative.

The purpose of principles policies and procedures is to convey the governing bodies and management's direction and instructions. They are instruments to communicate the rules of the enterprise, in support of the governance objectives and enterprise values as defined by the board and executive management. The primary reason for implementing principles, policies and procedures is to translate the desired strategy into practical guidance for day-to-day management. The key difference between principles and policies are that principles need to be limited in number. The characteristics of good policies are that they should:

- Be effective: achieve their purpose
- Be efficient: especially when implementing them
- Non-intrusive: Should make sense and be logical to those who have to comply with them.

Policies should have a mechanism (framework) in place where they can be effectively managed, and users know where to go. Specifically, they should be:

- Comprehensive, covering all required areas
- Open and flexible allowing for easy adaptation and change.
- Current and up to date

The purpose of a policy life cycle is that it must support a policy framework in order to achieve defined goals and express clearly as possible the core values of the enterprise. Policies are more detailed guidance on how to put principles into practice. The good practice requirements for policies and procedures have to be approved by the Board and senior management. These are important and should specifically cover the following:

- Scope and applicability.
- Consequences of failing to comply with the policy.
- Means of handling exceptions.
- How they will be monitored.

The links and relationships between principles, policies, Procedures and other components are:

- Principles, policies and Procedures reflect the cultures, ethics and values of the enterprise.
- Processes are the most important vehicle for executing policies.
- Organizational structures can define and implement policies.
- Policies are part of information which has to be documented and communicated.

3.3.2 Processes

The second component of COBIT 2019 is "Processes". *A process is defined* as 'a collection of practices influenced by the enterprises policies, and procedures that takes inputs from a number of sources (including other processes) manipulates the inputs and produces outputs (e.g. products and services).

- *Process practices* are defined as the 'guidance' necessary to achieve process goals.
- *Process activities* are defined as the 'guidance' to achieve management practices for successful governance and management of enterprise IT.
- *Inputs and Outputs* are the process work products/artefacts considered necessary to support operation of the process.

Process model of COBIT 2019 focuses on generic processes required by organization to implement within organization. It clearly distinguishes between Governance processes and management processes.

Each process should provide:

- Process description
- Process purpose statement
- IT-related Goals
- Each IT-related goal is associated with a set of generic related metrics
- Process Goals (also from the Goals cascade mechanism and is referred to as Component Goals).
- Each process goal is associated or related with a set of generic metrics.
- Each Process contains a set of Management Practices.
- These are associated with a generic RACI chart (Responsible, Accountable, Consulted, Informed)
- Each management practices contains a set of inputs and outputs (called work products)
- Each management Practice is associated with a set of activities.

In addition, COBIT 2019 identifies the goals for each process and also defines the metrics to measure the performance of each process.

3.3.3 Organizational Structures

The third component of COBIT 2019 is "Organisational structures". Establishing accountability mechanisms through appropriate organisation structure is the corner-stone of governance implementation. Deployment of IT requires involvement not only from management (management processes) but also from the Board of directors (governance processes).

Hence, the organisation structure has to include establishing specific responsibility for both governance and management. The key role and responsibilities for most of the typical functions in an organisation from governance and management perspective is identified for each of the 200+ management practices covering all the 40 Governance and Management objectives. This is provided in the RACI chart which will help in defining roles, responsibilities covering risks and controls for all critical areas as per COBIT 2019 processes and practices. Using these practices will help organisations to establish a number of good practices of organizational structure such as:

- Operating Principles: The practical arrangements regarding how the structure will operate, such as meeting frequency documentation and other rules
- Span of Control: The boundaries of the organization structure's decision rights.
- Level of Authority: The decisions that the structure is authorized to take.
- Delegation of Responsibility: The structure can delegate a subset of its decision rights to other structures reporting to it.
- Escalation Procedures: The escalation path for a structure describes the required actions in case of problems in making decisions.

An organization structure shall vary from organization to organization depending on the level of authority, responsibility and span of control. A generic structure may look like the following diagram:

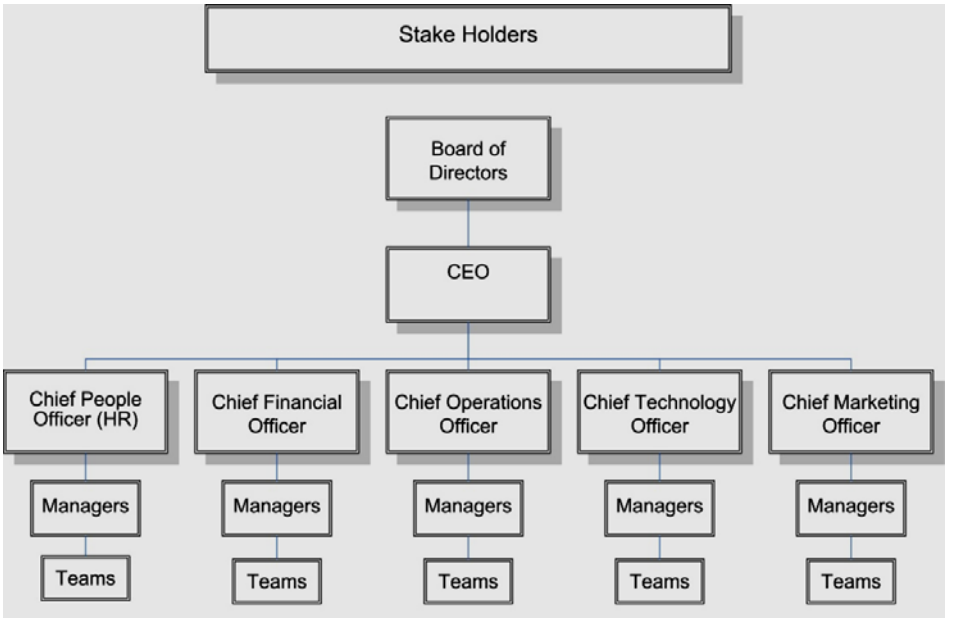

Figure 3.3: Organization Structure

Fundamentally, the role of an IT department within an organisation is to design, maintain, and support an organisation's information technology infrastructure, thus allowing the organisation to leverage both information and technology in an efficient, productive and secure manner. The IT Organizational Structure also aims at supporting the organization in its future growth and evolutionary process, as can be seen from the pictorial representation below:

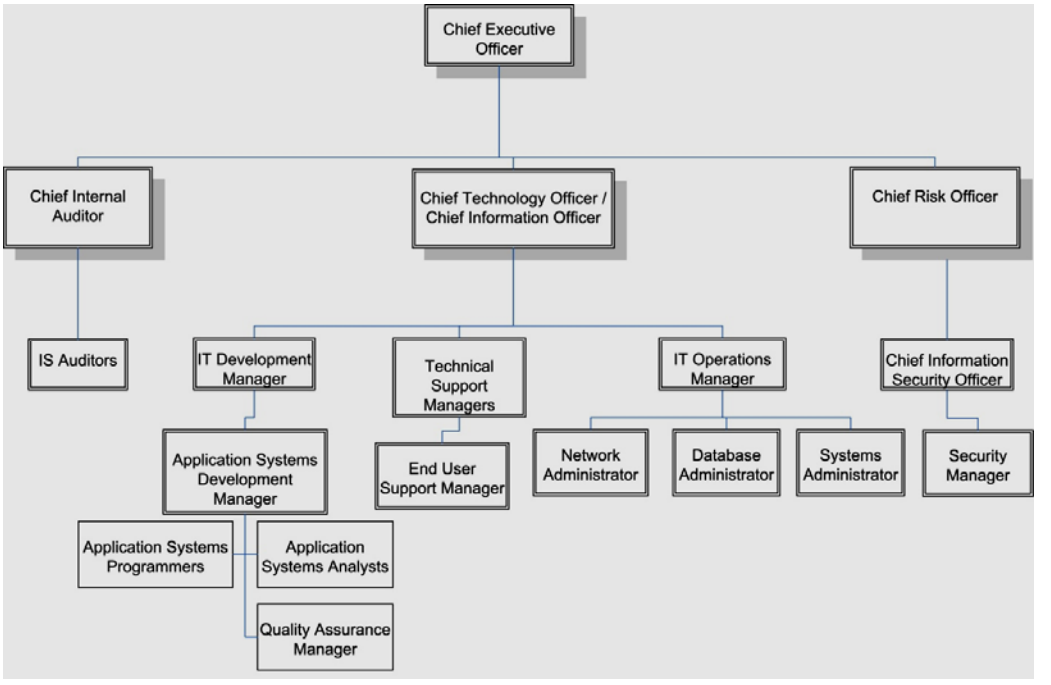

Figure 3.4: Organization Structure of IT Department

Implementing right organisation structure from governance perspective requires creation of the right accountability mechanisms and decision-making system. This requires establishing committees at different levels covering all areas right from strategy to execution. Two important committees which are required for implementing effective EGIT are the IT Strategy committee and the IT Steering Committee. The roles and responsibilities of each of these committees is explained below.

3.3.3.1 IT Strategy Committee

Enterprise Governance of I&T should be an integral part of corporate governance, and in this way a primary concern of the board of directors. Boards may carry out their governance duties through committees and they can consider the criticality of IT through an IT strategy committee. The IT strategy committee is composed of board and non-board members. They should assist the board in governing and overseeing the enterprise's IT-related matters. This

committee should ensure that IT is a regular item on the board's agenda, where it must be addressed in a structured way. The IT strategy committee should work in close relationship with the other board committees and with management in order to provide input to, and to review and amend the aligned enterprise and IT strategies. The implementation of the IT strategy must be the responsibility of executive management assisted by one or more IT steering committees. Typically, such a steering committee has the responsibility for overseeing major projects and managing IT priorities, IT costs, and IT resource allocation. While the IT strategy committee operates at the board level, the IT steering committee is situated at executive level, which implies that they have different responsibility, authority and membership

3.3.3.2 IT Steering Committee

Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives. As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee. Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management. As the members comprise of function heads of departments, they would be responsible for taking decisions relating to their departments as required. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. The key functions of the committee would include:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;

- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

Appointment: The IS Steering Committee is appointed by the Board in order to oversee the IS Department's processes, and it operates at the executive level.

Responsibilities: The duties, responsibilities, authority and accountability of the Steering Committee should be defined in a formal charter, which should be approved by the Board. Members should know IS department policies, practices and procedures. Each member should have the authority to make decisions within the group for his or her respective areas.

Objective: The primary objective of the Steering Committee is to ensure that the IS department is aligned with the organization's mission and objectives. It provides planning and control for the organization's IS function.

Chairman: It should preferably be chaired by a member of the board of directors who understands information technology risks and issues.

Representation: The membership of the committee should be broad-based and should include a cross-section of senior business managers including legal and finance, senior management, user management and IS department.

Clear job definitions have to be provided for all key IT positions so as to ensure that the required IT organisation structure is established. It is also important to understand the roles, responsibilities and risks of key IT personnel.

3.3.4 Culture, Ethics and Behavior

The fourth component of COBIT 2019 is "Culture, ethics and Behavior". The principles of this component are inbuilt in the processes and other guidance. Organizational Ethics determine the values by which the enterprise want to live (its code). Individual ethics determined by each person's personal values and dependent to some extent on external factors not always under the enterprise's control. Individual behaviours which collectively determine the culture of the enterprise and is dependent on both organizational and individual ethics. In governance terms, culture is significantly influenced but what is referred to as "The Tone from the Top". In other words, the spoken and unspoken messages sent from the IT executive leadership, which in turn influences managerial behaviour and directly influences company plans, policies, and organizational direction. In short, culture is shaped and transformed by consistent patterns of senior management action. Some examples are:

- Behaviour towards risk taking
- Behaviour towards the enterprise's principles and policies
- Behaviour towards negative outcomes, e.g. loss events

Good practices for creating, encouraging and maintaining desired behaviour throughout the enterprise include:

- Communication throughout the enterprise of desired behaviours and corporate values. (This can be done via a code of ethics).
- Awareness of desired behaviour strengthened by senior management example. This is one of the keys to a good governance environment when senior management and the executives 'walk the talk' so to speak. It is sometimes a difficult area and one that causes many enterprises to fail because it leads to poor governance. (Typically, this will be part of a training and awareness sessions based around a code of ethics).
- Incentives to encourage and deterrents to enforce desired behaviour. There is a clear link to HR payment and reward schemes.
- Rules and norms which provide more guidance will typically be found in a Code of Ethics.

3.3.5 Information

Information is the fifth component of COBIT 2019. Information is processed using information technology. The success of an enterprise in the digital world depends on how well information is harnessed for achieving enterprise objectives. Information is the most valuable asset and success of an enterprise is determined by how well information is processed and made available to all the stakeholders with the requisite level of security. Ensuring the right type of information using information systems in safe and secure environment is the most critical aspects of technology deployment. As per COBIT 2019, Information is currency of the 21st century. Process requires information and management at all levels require information for decision making and monitoring performance. IT maintains information and hence the attributes of information are most important for business and management. IT supports business process by generating and processing data. The information is then transformed into knowledge that creates value for management and helps in decision which affects the business process. The attributes required to assess the context and quality of information to the user which need to be considered, specifically are:

- Relevancy: The extent to which information is applicable and helpful for the task at hand
- Completeness: The extent to which information is not missing and is of sufficient depth and breath for the task at hand
- Appropriateness: The extent to which the volume of information is appropriate for the task at hand.
- Conciseness: The extent to which the information is compactly represented.
- Consistency: The extent to which the information is presented in the same format.

- Understandability: The extent to which the information is easily understandable
- Ease of Manipulation: The extent to which information is easy to manipulate and apply to different tasks.

3.3.6 Services, Infrastructure and Applications

The sixth component of COBIT 2019 is: "Services, infrastructure and Applications". This refers to the services provided by IT to business and stakeholders to meet internal as well as external requirements. Application helps in providing services by processing information. Application is hosted using IT infrastructure. Application software are at the heart of processing of transaction processing and encompass all mission critical processes. In a modern enterprise where services are provided an on-line, real-time basis, services, infrastructure and applications provide the most critical foundation for providing services to customers. Hence all these three aspects: services, infrastructure and applications must be considered together. Modern applications are complex and interacts with various technologies, for example core banking application is hosted on server that processes and provide data in real time to various delivery channels likes ATM, Mobile banking, Internet banking, Branch banking. All delivery channels are set of applications focusing on providing services to customers. Hence a bank must consider all these three objects together.

There are five architecture principles that govern the implementation and use of I&T-Related resources. This is part of the good practices of this component. Architecture principles are overall guidelines that govern the implementation and use of I&T-related resources within the enterprise. Examples of such principles are:

- Reuse: Common components of the architecture should be used when designing and implementing solutions as part of the target or transition architectures.
- Buy vs. Build: Solutions should be purchased unless there is an approved rationale for developing them internally.
- Simplicity: The enterprise architecture should be designed and maintained to be as simple as possible while still meeting enterprise requirements.
- Agility: The enterprise architecture should incorporate agility to meet changing business needs in an effective and efficient manner.
- Openness: The enterprise architecture should leverage open industry standards.

The services, infrastructure and applications as an component is also designed and built based on the IT strategic plan which in turn is derived from the enterprise strategic plan. For most enterprises, the investment and cost of this component would be the highest and hence needs to be managed both as a one-time projects and as on-going maintenance projects as relevant. Any new business initiative would require IT enabled change which has to be supported by required services, infrastructure and applications and once deployed, there is a need for on-going maintenance to ensure that the required level of services is provided.

3.3.7 People, Skills and Competencies

People, Skill and competencies are the most valuable asset of an enterprise. In an increasingly digital world where most of the routine transaction processing is automated. It is the people with the required skills and competencies who are the key differentiator. IT is only enabler and by itself provide value. Value is derived by how IT is harnessed through right blend of people, process and technology. It is the employees of an enterprise who as knowledge workers use the power of IT to provide services to customers. In the service industry, the human resources are the most valuable asset. Technology can be bought but effective implementation requires people to be trained with the requisite skills and competencies to provide services. Nothing can move unless supported and managed by people who use their intrinsic capacity to analyze information and take decisions. Without people organizations will not exist. People, however, possess different skills and organization need people with different skills. In order to ensure appropriate skills organization, follow various people management practices like training, motivational programs, career progressions, job rotation.

While defining organization structure organizations also define job description, roles and responsibilities along with competencies required to perform the job. For example, IT related activities likes business analysis, system design, development and coding, testing. Organizations also consider outsourcing to ensure appropriate skill and competencies are available to achieve performance and service delivery objectives. For implementing EGIT, organizations require skills for developing and executing IT Policy formulation, IT strategy, enterprise architecture, innovation, financial management, portfolio management and many such related processes as relevant.

The seven components of COBIT 2019 have to be implemented in enterprises of all sizes regardless of nature of business or sector or technology deployment. However, the relevance of each these components would vary across enterprises. For example, in a software company, the component: people, skills and competencies are extremely important whereas in the case of highly regulated industry, the component: culture, ethics and behavior is most important. For successful implementation of EGIT, selecting the right blend of these components customised as required is most critical. The components also have the openness of integrating across various frameworks.

3.4 Designing a Tailored Governance System of COBIT 2019

Effective governance over information and technology is critical to business success. The design guide is a new offering that includes four steps to design a tailored governance system:

1. Understand the enterprise context and strategy. This includes understanding the enterprise strategy, goals, risk profile, and current information- and technology-related challenges.

2. Determine the initial scope of the governance system. This includes establishing governance and management priorities.
3. Refine the scope of the governance system. This includes considering the threat landscape, compliance requirements, the role of IT, the technology adoption strategy, enterprise size and more.
4. Conclude the governance system design. This includes resolving priority conflicts, adopting resolution strategies and conclude the governance system design.

3.5 Stakeholders in Implementing EGIT

There are many stakeholders who need to collaborate to achieve the overall objective of improved IT performance. The most important stakeholders and their specific role and responsibilities are outlined here:

- Board and executive management: How do we set and define enterprise direction for the use of I&T and monitor that relevant and required *EGIT* enablers are established so that business value is delivered, and I&T-related risks are mitigated?
- Business management and business process owners: How do we enable the enterprise to define/align I&T-related goals to ensure that business value is delivered from the use of I&T and I&T-related risks are mitigated?
- Chief information officer (CIO), IT management and IT process owners: How do we plan, build, deliver and monitor information and IT solutions and service capabilities as required by the business and directed by the board?
- Risk, compliance and legal experts: How do we ensure that we are in compliance with policies, regulations, laws and contracts, and risks are identified, assessed and mitigated?
- Internal audit: How do we provide independent assurance on value delivery and risk mitigation?

3.6 Using Systematic Approach for Implementing EGIT

COBIT 2019: Implementation provides a systematic approach for implementing EGIT project within an enterprise with specific phases, tasks and activities and roles and responsibilities and deliverables of each of these phases. One of the key components of EGIT implementation is “Culture, ethics and behavior”. This is set by the tone at the top with the senior management establishing and enforcing the right culture. In implementing EGIT, this is most critical. The overall enterprise environment should be analysed to determine the most appropriate change enablement approach. This will include aspects such as the management style, culture (ways of working), formal and informal relationships, and attitudes. It is also important to understand other IT or enterprise initiatives that are ongoing or planned, to

ensure that dependencies and impacts are considered. It should be ensured from the start that the required change enablement skills, competencies and experience are available and utilised: for example, by involving resources from the HR function or by obtaining external assistance. As an outcome of this phase, the appropriate balance of directive and inclusive change enablement activities required to deliver sustainable benefits can be designed. Brief overview of each of the phases of a EGIT implementation is provided. This approach has to be adapted as per requirements of the project.

3.6.1 Phase 1: Establish the Desire to Change

The purpose of this phase is to understand the breadth and depth of the envisioned change, the various stakeholders that are impacted, the nature of the impact on and involvement required from each stakeholder group, as well as the current readiness and ability to adopt the change. Current pain points and trigger events can provide a good foundation for establishing the desire to change. The 'wake-up call', an initial communication on the programme, can be related to real-world issues that the enterprise may be experiencing. Also, initial benefits can be linked to areas that are highly visible to the enterprise, which creates a platform for further changes and more widespread commitment and buy-in. While communication is a common thread throughout the implementation or improvement initiative, the initial communication or wake-up call is one of the most important and should demonstrate the commitment of senior management— therefore, it should ideally be communicated by the executive committee or CEO.

3.6.2 Phase 2: Form an Effective Implementation Team

Dimensions to consider in assembling the right core implementation team include involving the appropriate areas from business and IT as well as the knowledge and expertise, experience, credibility, and authority of team members. Obtaining an independent, objective view as provided by external parties, such as consultants and change agent, could also be highly beneficial and aid the implementation process or could address skill gaps that may exist within the enterprise. Therefore, another dimension to consider is the appropriate mix of internal and external resources. The essence of the team should be a commitment to:

- A clear vision of success and ambitious goals
- Engaging the best in all team members, all the time
- Clarity and transparency of team processes, accountabilities and communications
- Integrity, mutual support and commitment to each other's success
- Mutual accountability and collective responsibility
- Ongoing measurement of its own performance and the way it behaves as a team
- Living out of its comfort zone, always looking for ways to improve, uncovering new possibilities and embracing change

It is important to identify potential change agents within different parts of the business that the core team can work with to support the vision and cascade changes down.

3.6.3 Phase 3: Communicate Desired Vision

A high-level change enablement plan should be developed in conjunction with the overall programme plan. A key component of the change enablement plan is the communication strategy, which should address who the core audience groups are, their behavioural profiles and information requirements, communication channels, and principles. The desired vision for the implementation or improvement programme should be communicated in the language of those affected by it. The communication should include the rationale for and benefits of the change, as well as the impacts of not making the change (purpose), the vision (picture), the road map to achieving the vision (plan) and the involvement required of the various stakeholders (part). Senior management should deliver key messages (such as the desired vision). It should be noted in the communication that both behavioural/cultural and logical aspects should be addressed, and that the emphasis is on two-way communication. Reactions, suggestions and other feedback should be captured and acted upon.

3.6.4 Phase 4: Empower Role Players and Identify Quick Wins

As core improvements are designed and built, change response plans are developed to empower various role players. The scope of these may include:

- Organisational design changes such as job content or team structures
- Operational changes such as process flows or logistics
- People management changes such as required training and/or changes to performance management and reward systems

Any quick wins that can be realised are important from a change enablement perspective. These could be related to the pain points and trigger events discussed in previous chapter. Visible and unambiguous quick wins can build momentum and credibility for the programme and help to address any scepticism that may exist. It is imperative to use a participative approach in the design and building of the core improvements. By engaging those impacted by the change in the actual design, e.g., through workshops and review sessions, buy-in can be increased.

3.6.5 Phase 5: Enable Operation and Use

As initiatives are implemented within the core implementation life cycle, the change response plans are implemented. Quick wins that may have been realised are built on and the behavioural and cultural aspects of the broader transition are addressed (issues such as dealing with fears of loss of responsibility, new expectations and unknown tasks). It is important to balance group and individual interventions to increase buy-in and engagement and to ensure that all stakeholders obtain a holistic view of the change.

Solutions will be rolled out and during this process, mentoring and coaching will be critical to ensure uptake in the user environment. The change requirements and objectives that had been set during the start of the initiative should be revisited to ensure that they were adequately addressed. Success measures should be defined and should include both hard business measures and perception measures that track how people feel about a change.

3.6.6 Phase 6: Embed New Approaches

As concrete results are achieved, new ways of working should become part of the enterprise's culture and rooted in its norms and values ('the way we do things around here') - for example, implementing policies, standards and procedures. The implemented changes should be tracked, the effectiveness of the change response plans should be assessed, and corrective measures taken as appropriate. This might include enforcing compliance where still required. The communication strategy should be maintained to sustain ongoing awareness.

3.6.7 Phase 7: Sustain

Changes are sustained through conscious reinforcement and an ongoing communication campaign, and they are maintained and demonstrated by continued top management commitment. Corrective action plans are implemented, lessons learned are captured and knowledge is shared with the broader enterprise

3.7 Implementing EGIT in Specific Areas

Specific examples of implementing EGIT in specific areas are explained in the next section of this chapter. These cover key areas such as: Strategic alignment, value optimisation, resource optimisation, outsourcing and capacity management.

3.7.1 Strategic Alignment of IT with Business

Strategic alignment and performance measurement are important and apply overall to all the Governance and management activities to ensure that IT goals are aligned with the enterprise goals and there are process goals are set for the IT goals and metrics are designed for these. IT is a key enabler of corporate business strategy. Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chief Information Officers (CIO) agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives. Corporate governance drives the corporate information needs to meet business objectives. IT has to provide critical inputs to meet the information needs of all the required stakeholders or it can be said that enterprise activities require information from IT activities in order to meet enterprise objectives. Hence, corporate governance drives and sets I&T governance.

Management Strategy determines at the macro level the path and methodology of rendering services by the enterprise. Strategy outlines the approach of the enterprise and is formulated by the senior management. Based on the strategy adapted, relevant policies and procedures are formulated. From business strategy perspective, I&T is affecting the way in which enterprises are structured, managed and operated. One of the most dramatic developments affecting enterprises is the fusion of IT with business strategy. Enterprises can no longer develop business strategy separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business planning and the incorporation of effective financial and management controls within new systems. Management primarily is focused on harnessing the enterprise resources towards achievement of business objectives. This would involve the managerial processes of planning, organizing, staffing, directing, coordinating, reporting and budgeting.

3.7.1.1 Objective of IT Strategy

The primary objective of IT strategy is to provide a holistic view of the current I&T environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives. Alignment of the strategic IT plans with the business objectives is done by clearly communicating the objectives and associated accountabilities so they are understood by all and all the IT strategic options are identified, structured and integrated with the business plans as required.

IT organizations should define their strategies and tactics to support the organization by ensuring that day-to-day IT operations are delivered efficiently and without compromise. Metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of enterprise leaders. Internal audit can determine whether the linkage of IT metrics and objectives aligns with the organization’s goals, adequately measure progress being made on approved initiatives, and express an opinion on whether the metrics are relevant and useful. Additionally, auditors can validate that metrics are being measured correctly and represent realistic views of IT operations and governance on a tactical and strategic basis.

3.7.1.2 IT Strategic Planning

The strategic planning process has to be dynamic in nature and IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the enterprise's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long and short-range plan are developed and maintained. IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT

conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

3.7.2 Aligning IT Strategy with Enterprise Strategy

The key management practices, which are required for aligning IT strategy with enterprise strategy, are highlighted here:

- Understand enterprise direction: Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- Assess the current environment, capabilities and performance: Assess the performance of current internal business and IT capabilities and external IT services and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- Define the target IT capabilities: Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- Conduct a gap analysis: Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- Define the strategic plan and road map: Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- Communicate the IT strategy and direction: Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals,

extent of stakeholder satisfaction with scope of the planned portfolio of programs and services and the percentage of IT value drivers, which are mapped to business value drivers.

3.7.3 Value Optimization

Business value from use of I&T is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from I&T-enabled investments at an acceptable cost. The benefit of implementing this process will ensure that enterprise is able to secure optimal value from I&T-enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

The success of the process of ensuring business value from use of I&T can be measured by evaluating the benefits realized from I&T enabled investments and services portfolio and how transparency of IT costs, benefits and risk is implemented.

3.7.3.1 Metrics for value optimization

Some of the key metrics, which can be used for such evaluation, are:

- Percentage of I&T enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where expected benefits realized;
- Percentage of I&T enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT-related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of I&T financial information.

3.7.4 Resource Optimization

The process of Resource optimisation has to be implemented to ensure that adequate and sufficient I&T related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost. The primary objectives of implementing this process is to ensure that the resource needs of the enterprise are met in the most optimal manner, I&T costs are optimised, and there is an increased likelihood of benefit realization and readiness for future change. A key to successful I&T performance is the optimal investment, use and allocation of I&T resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise.

3.7.5 Sourcing Processes

Sourcing is managed through suppliers and appropriate service agreements.

Sourcing processes refer to the procurement practices of an organization in order to find, evaluate and engage vendors of goods and services. The purchasing processes should ensure that the processes are defined and capable of meeting organizational needs. This involves several activities like:

- Timely identification of needs.
- Evaluation of product cost, performance and delivery and installation logistics.
- Method of evaluating that quality needs have been met.
- Contract administration, guarantee replacement or warranty, access to the vendors premises, vendor development and
- Reduction of vendor related risks.

3.7.6 Outsourcing

Outsourcing is a strategic decision for management in order to achieve long-term improvement in business performance, by utilising the vendor's core competencies. IT is one of the key areas which is outsourced in part or in totality depending on the criticality of the processes. Although IT outsourcing has many benefits, it has inherent risks which need to be mitigated. The risks are much more when IT outsourcing covers strategic use of IT. Hence, mitigating these risks require all the service provider are managed through an appropriate structure. This vendor management process should not only monitor performance but also include specific functional heads who have the appropriate level of authority to hold the service providers accountable. Some of the important tools which are used to manage, and monitor IT service providers are performance targets, service level agreements (SLAs), and scorecards. It is critical to note that senior management cannot abdicate its ultimate responsibility for IT service delivery just because it has been outsourced as the responsibility for compliance and ensuring performance vests with the enterprise. The key principles and guidelines as explained earlier relating to sourcing are applicable to outsourcing as this is also a form of sourcing.

3.7.7 Capacity Management & Growth Planning Processes

Capacity management is the process of planning, sizing and continuously optimising IS capacity in order to meet long and short-term business goals in a cost effective and timely manner. Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner. Capacity management to be effective has to be supported by an effective process of monitoring and evaluating Performance and Conformance. The scope of this process is to collect, validate and evaluate business, IT and

process goals and metrics. Monitor that processes are performing against agreed performance and conformance goals and metrics and provide reporting that is systematic and timely. This helps in providing transparency of performance and conformance and drive achievement of goals. Capacity management or configuration management process is used in order to assess the effectiveness and efficiency of the IS operations. Capacity includes:

- Storage space
- Network throughput
- Human resources
- Electronic messaging
- Customer Relationship Management
- Quantum of data processed, etc.

The benefits of good capacity management are:

- Enhanced customer satisfaction
- Better justification of spending on IS resources
- Avoiding incorrect capacity sizing which may lead to inappropriate utilisation of IS resources and insufficient capacity to process the production workloads
- A reduction in capacity failures
- Better alignment of business needs and IS resources
- Better service level management

3.7.8 Capex and Opex

Outsourcing and capacity management requires effective utilisation of resources thereby resulting in business value from investments. In the current era, IT is being regarded increasingly as a utility and there are vendors providing all types of IT outsourcing services. Use of IT through outside vendors reduces capital expenditure but increases revenue expenditure or it can be said that Capex is converted to Opex. It is important for management to understand the key concepts of Capex and Opex as they impact the funds outflow and ROI on usage of such IT resources. These concepts are briefly explained here.

Capex stands for Capital Expenditures and is the money spent of generating physical assets. Opex stands for Operating Expenditures and refers to day to day expenses required to maintain physical assets.

In general, Capex is what needs to be avoided, while Opex is something to be kept under tight control. Opex can be considered to be (in) efficiency of any business. It has a direct relation with the value of the business. If you can reduce Opex without hurting day to day operations, you eventually increase valuation of any business. The concept of Capex and Opex is critical to consider in making IT enabled investment decisions. The distinction between Capex and

Opex has become important as most of the organisations now look at outsourcing as the preferred option for all non-core activities. Further, in cloud computing environment, critical activities are outsourced by organisations considering the benefits of converting Capex into Opex. IS Auditors who are required to evaluate such alternatives have to consider not only the cost benefit analysis but also the associated risks and how these risks have been mitigated through implementation of appropriate controls.

3.7.9 Role of IS Auditors

IS auditors could be involved in providing assurance requiring review of Information Systems as implemented from control perspective. However, auditors may also be required to provide consulting before, during or after implementation of information systems strategy. It becomes imperative for the auditor to understand the concepts of the enterprise strategy as relevant. Hence, auditors must have good understanding of management aspects as relevant to deployment of I&T and IT strategy. This would include understanding of the IS Strategy, policies, procedures, practices and enterprise structure, segregation of duties, etc.

3.8 Summary

The seven key components for implementing EGIT are the building blocks for any technology deployment. This chapter has provided details of key characteristics of each of the seven components. These seven components are: Principles, policies, Procedures Processes, Information, Organizational structures, Services, infrastructure and applications, People, skills and competencies and Culture, ethics and behavior. Each of these components is critical. However, information is most valuable for most of the enterprises. Each of these enables have their own characteristics that have to be considered while implementing EGIT. Organization need to ensure that these components are implemented as appropriate depending on the requirements of the organization.

In implementing EGIT, it is most important to note that Governance and management are different concepts. Governance is providing direction and monitoring performance, whereas management is about implementing, executing and monitoring activities as per the strategy to ensure that enterprise objectives are achieved. How well these components are effective would also depend on the involvement of senior management with the governance perspective of providing direction and channelizing use of technology from strategic perspective. COBIT 2019 provides generic guidance for each of these components and in case of processes and information, there are specific publications which provide detailed guidance. However, implementation of these seven components requires integration and use of detailed guidance from other relevant frameworks as required. However, considering that COBIT 2019 is an umbrella framework, it provides the overall framework for integration of best practice guidance from all frameworks.

3.9 Questions

1. Which of the following is most important resource of the organization?
   A. Policies and procedures
   B. IT infrastructure and applications
   C. Information and data
   D. Culture, ethics and behaviour
2. Which of the following is most important characteristic of policies?
   A. Must be limited in number.
   B. Requires framework to implement.
   C. Reviewed periodically.
   D. Non-intrusive and logical.
3. Primary function of a process is to:
   A. Act on input and generate output.
   B. Define activities to be performed.
   C. Focus on achieving business goals.
   D. Comply with adopted standards.
4. Effective organizational structure focuses on:
   A. Defining designations.
   B. Delegating responsibility.
   C. Defining escalation path.
   D. Deciding span of control.
5. Prioritization of IT initiatives within organization is primarily based on:
   A. Results of risk assessments
   B. Expected benefit realization
   C. Recommendations of CIO
   D. Rate of obsolescence of IT
6. Primary objective of IT steering committee is to:
   A. Align IT initiatives with business
   B. Approve and manage IT projects
   C. Supervise IT and business operations

D. Decide IT strategy for organization

7. Which of the following is best control for building requisite skills and competencies within organization?

   A. Hiring only highly qualified people

   B. Outsourcing the critical operations

   C. Conducting skill enhancement training

   D. Defining skill requirements in job description

3.10 Answers and Explanations

1. C. Entire EGIT implementation focuses on Information and data. Policies are defined based on nature of information and data, culture and behaviour. IT infrastructure and applications stores, process and communicates information.

2. D. Policies are vehicle to communicate intent of management and hence must be clear and easy to implement that will make them effective. B and C are requirements to maintain policies and A is characteristic of principles.

3. A. Primary function of process is to process received inputs and generate output to achieve process goals. Process is a set of activities, but it is not primary function to define activities. Although processes are defined to achieve business goals, these are broken down to arrive at process goals. Compliance with standards may need certain processes but the primary function is to process input.

4. B. Effectiveness of organization structure depends on right level of delegation of responsibilities. Defining designation is only naming of specific role which is not directly relevant. Other options depend upon level of delegation.

5. B. Although the IT steering committee considers all inputs, the primary consideration is expected benefits to the organization.

6. A. The primary objective of appointing IT steering committee is to ensure that IT initiatives are in line with business objectives. D is objective of IT strategy committee. B and C are secondary objectives derived from A.

7. C. The best control for building requisite skills and competencies within organization is to ensure skill enhancement training is provided.

Chapter 4

Performance Management Systems

Learning Objective

The Governance processes of ISO 38500 and COBIT 2019 primarily focus on “Evaluate, Direct and Monitor”. Governance is an oversight function and evaluates the business environment in terms of the business strategy and objectives, the technology environment, market conditions, competitive environment, regulatory requirements and emerging innovations that could significantly impact and influence the business strategic and operating models of the organization.

The governance function thus provides the direction that the IT operation should integrate to maximize the support and involvement to the business. The governance function also monitors the performance of the IT operation in terms of its direction and the goals achieved. The ‘direct’ function provides what is expected from management, whereas ‘monitor’ function focuses on whether what was expected has been achieved or not. The challenge is to ‘evaluate’ what is actually achieved and validate whether it is as per set objectives. This evaluation should help enterprise to make a realistic assessment of what was achieved, what are the gaps and how to monitor the performance not only on reactive but proactive basis. This chapter provides an overview of key concepts and models of performance management system.

4.1 Introduction

An effective performance management system is the corner-stone for meeting this challenge and implementing effective governance. This requires setting goals and metrics which are integrated across all the key areas and are measured and monitored. The system of performance measurement can be implemented by use of relevant governance and performance frameworks such as balanced scorecards, maturity models, and quality systems. This chapter provides an overview of performance management systems with specific details of goals cascade from COBIT 2019 and also explains the principles of Balanced Scorecard and Strategic Scorecard.

4.2 Performance Measurement

Performance measurement is the process of collecting, analysing and/or reporting information regarding the performance of an individual, group, organization, system or component. It can involve studying the processes and strategies within organizations or studying enterprise processes, parameters and phenomena, to evaluate whether the results are in line with what was intended or should have been achieved. An important principle of

good governance is that management should provide direction using clearly defined and communicated objectives, and then manage adherence to objectives by applying appropriate practices. Monitoring of performance using metrics enables management to ensure that goals are achieved. In developing a performance management system, it is important to identify the enterprise goals and then obtain understanding of the connection between the entity's mission, vision and strategies and its operating environment.

The broad phases of performance measurement system are:

- Plan, establish and update performance measures
- Plan and establish the accountability of persons for the performance measures
- Collect and analyse data on performance
- Report on performance information and
- Take corrective action

Performance indicators or metrics will determine how well the process is performing in enabling the goals to be achieved. They are also indicators of capabilities and skills of IS personnel.

4.3 Performance Measurement System

To assess performance against set objectives, it is important to implement a performance management system which assesses performance against goals by setting right key goals indicators (KGI) and also implementing key process indicators (KPI) to monitor performance of process. Performance measurement system is one of the ways of monitoring and evaluating the business achievements. Getting business value from I&T and measuring that value are, therefore, important governance domains. They are responsibilities of both the business and IT and should take both tangible and intangible costs and benefits into account. In this way, good I&T performance management should enable both the business and IT to fully understand how I&T is contributing to the achievement of business goals, in the past and in the future. I&T performance management is aimed at identifying and quantifying I&T costs and I&T benefits. There are different monitoring instruments available, depending on the features of the costs and benefits.

Performance is evaluated at various levels such as: at organization level against goals and objectives, resource level against set performance goals by defining key performance indicators (KPI), risk level based on key risk indicators (KRI). There are two approaches for performance measurements:

1. Proactive approach where management implements measure to provide assurance on achieving goals by implementing best practices and using lead indicators.
2. Reactive approach were achievements are compared with goals using lag indicators.

4.4 Goal Setting

Goal setting is the first pre-requisite of performance management. This could be done at different levels of enterprise and each of these need to be integrated and linked together at all levels of the enterprise. At a macro level, the Board of directors set the enterprise direction and goals to be achieved. These are the overall enterprise goals and are derived from the enterprise strategy. The enterprise goals could be set from a top-down or bottom-up or combination of these two approaches. Typically, the top management sets the goal considering the views of the business units. Once the goals are set, the top-level goals need to be allocated to function/business units and specific goals set for each of them. From a governance perspective, the enterprise goals will have to be shared by the IT department which will prepare the IT strategy in alignment with the enterprise strategy. Based on the enterprise, the IT department will prepare the IT strategic plan and IT related goals. These IT goals facilitate achievement of enterprise goals.

A performance measurement system will broadly have two types of goals. These are:

- Outcome: These are called as goals and are evaluated through KGI (key goal indicators). The focus is on achieving the set results. These are also called lag indicators as the measurement of achievement is after the event or period.
- Performance: These refer to performance and are evaluated through KPI (key performance indicators). These are also called lead indicators as they measure the performance.

There are many approaches to performance management. In this chapter, we will understand some of the performance management practices based on COBIT 2019, Balanced Scorecard and Quality management.

4.4.1 Goal Setting and Stakeholder Needs

Understanding of current stakeholder needs relating to *EGIT* and current enterprise goals and how they impact *EGIT* is very helpful for three reasons:

- The stakeholder needs and enterprise objectives influence the requirements and priorities of *EGIT*. For example, there could be a focus on cost reduction, compliance or launching a new business product, each of which could put a different emphasis on current governance priorities.
- The stakeholder needs and enterprise objectives help to focus where attention should be given when improving *EGIT* and
- It assists the business and IT functions to do better forward pla*nnin*g of opportunities to add value to the enterprise.

4.4.2 Category of Enterprise Goal

Goals to be effective need to be covering all levels of operations of the enterprise. They also need to be linked and automated and used as a measure of evaluating how well the department or employees have performed. Enterprise goals could be categorised as per the table given below.

Table 4.1: Categories of Enterprise goals

Enterprise Goal Category	Relates to
Strategic	High-level goals, aligned with and supporting the enterprise's mission or vision
Operational	Effectiveness and efficiency of the enterprise's operations, including performance and profitability goals, which vary based on management's choices about structure and performance.
Reporting	The effectiveness of the enterprise's reporting, including internal and external reporting and involving financial or nonfinancial information.
Compliance	The enterprise's compliance with applicable laws and regulations.

Enterprise goals are set by the board of directors based on the strategy and objectives. The list of enterprise goals are given here. These need to be customised by selecting by what is relevant for the enterprise and adding specific dates, values and number to the identified goals. Enterprise goals include:

- EG01: Portfolio of competitive products and services
- EG02: Managed business risk
- EG03: Compliance with external laws and regulations
- EG04: Quality of financial information
- EG05: Customer-oriented service culture
- EG06: Business service continuity and availability
- EG07: Quality of management information
- EG08: Optimization of business process functionality
- EG09: Optimization of business process costs
- EG10: Staff skills, motivation and productivity
- EG11: Compliance with internal policies
- EG12: Managed digital transformation programs
- EG13: Product and business innovation

4.4.3 Enterprise and Alignment Goals

Enterprise and alignment goals are used as the basis for setting IT objectives and for establishing a performance measurement framework. IT objectives are expressed as goals and need to be aligned with enterprise goals. COBIT 2019 provide structures for defining goals at three levels: for the enterprise, for IT overall, for IT processes. These goals are supported by metrics known as outcome measures because they measure the outcome of a desired goal. The metrics at a specific level also act as performance drivers for achieving higher-level goals. These goals and metrics can be used to set objectives and monitor performance by establishing scorecards and performance reports as well as for driving improvements.

The list of alignment goals are given here. These need to be customised by selecting by what is relevant for the enterprise and adding specific dates, values and number to the identified goals. Alignment goals include:

AG01: I&T compliance and support for business compliance with external laws and regulations

- AG02: Managed I&T-related risk
- AG03: Realized benefits from I&T-enabled investments and services portfolio
- AG04: Quality of technology-related financial information
- AG05: Delivery of I&T services in line with business requirements
- AG06: Agility to turn business requirements into operational solutions
- AG07: Security of information, processing infrastructure and applications, and privacy
- AG08: Enabling and supporting business processes by integrating applications and technology
- AG09: Delivering programs on time, on budget and meeting requirements and quality standards
- AG10: Quality of I&T management information
- AG11: I&T compliance with internal policies
- AG12: Competent and motivated staff with mutual understanding of technology and business
- AG13: Knowledge, expertise and initiatives for business innovation

4.5 Requirements for Measures

Measures and performance information need to be linked to strategic management processes. An effective performance management system produces information that provides following benefits:

- It is an early warning indicator of problems and the effectiveness of corrective action.
- It provides input to resource allocation and planning. It can help enterprises prepare for future conditions that are likely to impact program and support function operations and the demands for products and services, such as decreasing personnel or financial resources or changes in work load. Use of measures can give organizations lead times for needed resource adjustments, if these conditions are known in advance.
- It provides periodic feedback to employees, customers and stakeholders about the quality, quantity, cost and timeliness of products and services.

The most important benefit of setting measures is that it builds a common results language among all decision makers. Selected measures define what is important to an enterprise, what it holds itself accountable for, how it defines success and how it structures its improvement efforts.

4.5.1 Performance Measurement Processes / Indicators

This is considered to be an important part of the I&T governance processes. They say that what cannot be measured cannot be improved on. Therefore, metrics should be generated for e.g. all products and processes, financial measurement, benchmarking and external party evaluation, satisfaction of customers, internal staff and stakeholders, in order to ensure that they are achieving the desired results. Performance measurement is used to:

- Measure and manage products and services
- Assure accountability
- Make budgeting decisions and
- Optimise performance i.e. improve the productivity of IS to its highest possible level without making unnecessary added investments in the IS infrastructure.

Performance indicators or metrics will determine how well the process is performing in enabling the goals to be achieved. They are also indicators of capabilities and skills of IS personnel.

4.5.2 Examples of Performance Measures

- Better use of communications bandwidth and computing power
- Lower number of non-compliance with prescribed processes reported
- Better cost and efficiency of the process
- Lower numbers of complaints made by stakeholders
- Better quality and increased innovation etc.
- Lower number of errors and rework
- Improved staff productivity

4.5.3 Measures Defined

In the context of EGIT, goals and metrics are defined at three levels:

1. Enterprise goals and metrics: Define the organizational context and objectives and how to measure them
2. Alignment goals and metrics: Define what the business expects from IT and how to measure it
3. Governance and management objectives and metrics: Define what the IT-related process must deliver to support IT's objectives and how to measure it

In these three levels, it is important to make a distinction between outcome measures and performance drivers. Outcome measures indicate whether goals have been met. These can be measured only after the fact and, therefore, are sometimes called lag indicators.

4.6 Balanced Scorecard (BSC)

A Balanced Scorecard, as defined by Robert S. Kaplan and David P. Norton, groups objectives, measures, targets, and initiatives into four perspectives: financial, customer, learning and growth, and internal processes. The BSC focuses the energy of an organization into achieving strategic goals and objectives that are represented by key performance indicators (KPIs) customized to every group or business unit of the organisation. BSC is a methodology to solve challenges in balancing the theories of a strategy with its execution. BSC has the following characteristics:

- The methodology is suitable for managing business strategy.
- Uses a common language at all levels of the organization.
- Uses a common set of principles to manage day-to-day operations as well as to framework the organization's strategy.
- Designed to identify and manage business purposes.
- Provides a balance between certain relatively opposing forces in strategy:
    - Internal and external influences
    - Leading and lagging indicators and measures
    - Financial and non-financial goals
    - Organizational silos focused on their own goals and an over- arching framework of goals
    - Finance priorities and operations
- Aligns strategic goals with objectives, targets, and metrics.

4.6.1 BSC Perspectives

The four perspectives of BSC with examples are explained here.

1. Financial Perspective. The Financial perspective contains measures that indicate whether a strategy is achieving bottom-line results. Financial metrics are classic lagging indicators. The more common ones are:

- Profitability
- Revenue growth
- Economic value added

2. Customer Perspective. The Customer perspective defines the organization's target customers and the value proposition it offers them, whether it is efficiency (low price, high quality), innovation, or exquisite service. Most customer metrics are lagging indicators of performance, as follows:

- Customer satisfaction
- Customer loyalty
- Market share, "share of wallet"

3. Internal Process Perspective. Delivering value to customers involves mastering numerous internal processes, including product development, production, manufacturing, delivery, and service. Organizations may need to create brand new processes to meet goals outlined in the Customer perspective. Common metrics are:

- Patents pending, ratio of new products to total products
- Inventory turnover, stock-outs
- Zero defects, on-time deliveries

4. Learning and Growth Perspective. This perspective measures the internal resources needed to drive the other three perspectives. These include employee skills and information technology. Typical metrics are:

- Employee satisfaction, turnover rate, absenteeism
- Training hours, leadership development programs
- Number of cross-trained employees, average years of service

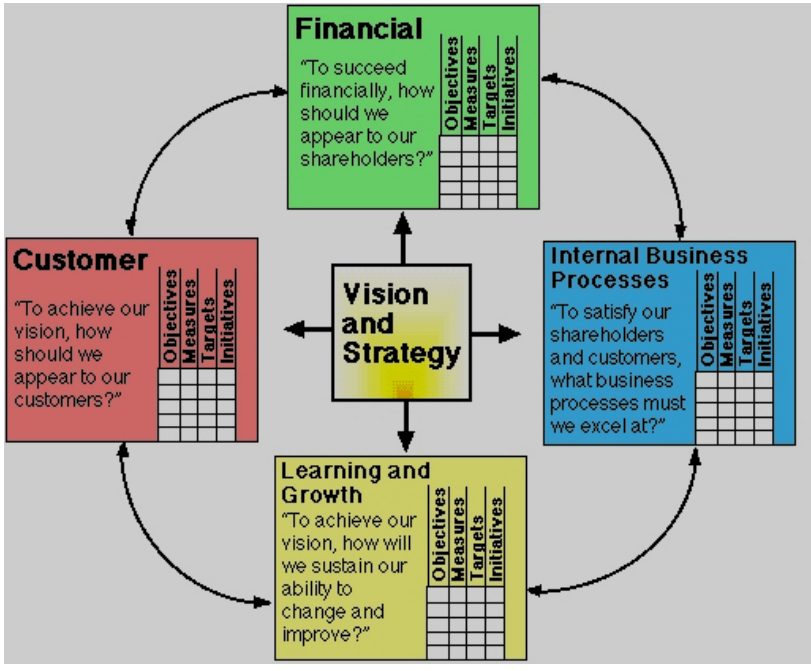

Figure 4.1: The Balanced Scorecard

BALANCED SCORECARD EXAMPLE – CREDIT CARD COMPANY

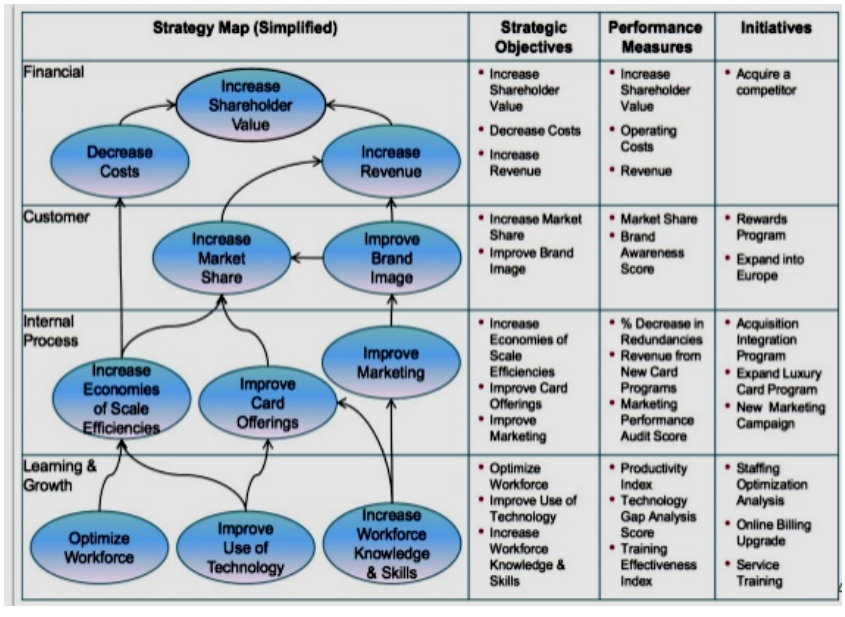

Figure 4.2: Balanced Scorecard example

4.7 Strategic Scorecard

The CIMA (Chartered Institute of Management Accountants) Strategic Scorecard is a pragmatic and flexible tool that is designed to help boards to fulfil their responsibilities to contribute to and oversee strategy effectively. It is the responsibility of the management team to develop and propose the strategy. However, it is not for the board to undertake the detailed strategic planning. The board's focus should be to challenge the strategy constructively, endorse it and monitor its implementation. The implementation of the scorecard assumes that the organization has already determined its broad strategic direction and has a strategic plan in place. The scorecard represents a process for developing and moving this strategy forward in a dynamic way.

The enterprise governance framework helps understand the importance of both conformance and performance to the organization's long-term success. What the scorecard does is to give the board a simple, but effective process that helps it to focus on the key strategic issues and – most importantly – to ask the right questions. This means that the board can work constructively with management to promote the future success of the organization. The uniqueness of the scorecard lies in the fact that it:

- Summarizes the key aspects of the environment in which an organization is operating to ensure that the board is aware of changing competitor, economic and other factors.
- Identifies the (key) strategic options that could have a material impact on the strategic direction of the organization and helps the board to determine which options will be developed further and implemented.

The primary objectives of using the strategic scorecard are:

- Assist the board in the oversight of a strategic process
- Deal with the strategic choice and transformational change
- Give a true and fair view of the company's strategic position and progress
- Track the actions into and out from the strategic process
- At the heart of the framework is the argument that good corporate governance can help to prevent failure, but it does not guarantee good business performance.

The Strategic Scorecard has four basic elements (Figure 4.3) aimed at helping the board to ensure that all strategic aspects are covered by making the board aware of what work is being done.

Figure 4.3: Strategic Scorecard

1. Strategic Position deals with information on:

- The micro environment e.g. market, competition and customers
- The macro environment e.g. political, economic and regulatory factors
- Threats from changes e.g. strategic inflexion points
- Business position e.g. market share, pricing, quality, service
- Capabilities e.g. core competencies and SWOT analysis which deals with Strengths, Weaknesses, Opportunities and Threats
- Stakeholders e.g. vendors, employees, shareholders

2. Strategic Options deals with what options are available with respect to:

- Scope change e.g. area, product, market sector
- Direction change e.g. high or low growth, price and quality offers

3. Strategic Implementation deals with:

- Project milestones and timelines
- Pursue or abandon the plan etc.

4. Strategic Risks deals with what can go wrong and what must go right with respect to:

- Informing the board on risks and how they are being managed
- Measurement of risks
- Internal controls

4.8 Summary

The purpose of performance measurement is to uncover, communicate and evolve organizational performance drivers. The choice of measures communicates to stakeholders what is important, and this affects what gets done. Choosing measures that answer critical management questions improves management's visibility into key processes. This chapter has provided an overview of performance management system with specific details from COBIT 2019 using enterprise goals, alignment goals with examples of specific process with alignment goals with related metrics and process goals with related metrics. Further, the key concepts of Balanced score card with the four perspectives with example have been illustrated.

The key to success is setting goals and monitoring them to ensure success with corrective steps to be taken as required. Use of frameworks helps in setting the right goals with the metrics to measure and monitor successful achievement of the goals. Performance measurement is critical for successful implementation of Governance or EGIT. Performance management helps management in keeping on track towards meeting stakeholder requirements and also in complying with regulatory requirements on time. IS Auditors with knowledge of performance management system can provide assurance or advisory services on the performance management system in place and provide recommendations for improving the effectiveness.

4.9 Questions

1. Which of the following is best approach for monitoring the performance of IT resources?
    A. Compare lag indicators against expected thresholds
    B. Monitor lead indicators with industry best practices
    C. Define thresholds for lag indicators based on long term plan
    D. Lead indicators have corresponding lag indicator.
2. Performance monitoring using balance score card is most useful since it primarily focuses on:
    A. Management perspective
    B. Product and services
    C. Customer perspectives
    D. Service delivery processes
3. Which of the following is considered as an example of a lead indicator?
    A. Number of gaps with respect to industry standard.
    B. Comparative market position of organization.

C. Percentage of growth achieved over three years.

D. Improvement in customer satisfaction survey.

4. The PRIMARY objective of base lining IT resource performance with business process owners is to:

A. define and implement lead and lag indicators.

B. ensure resource planning is aligned with industry.

C. assess cost effectiveness of outsourcing contracts.

D. benchmark expected performance measurement.

5. Which of the following is BEST measure to optimize performance of skilled IT human resources?

A. Include personal development plan in job description.

B. Document personal expectations during exit interviews.

C. Implement 'Bring Your Own Device (BYOD)' policy.

D. Monitor performance measure against baseline.

6. IT resource optimization plan should primarily focus on:

A. Reducing cost of resources

B. Ensuring availability

C. Conducting training programs

D. Information security issues

7. The PRIMARY objective of implementing performance measurement metrics for information assets is to:

A. decide appropriate controls to be implemented to protect IT assets.

B. compare performance of IT assets with industry best practices.

C. determine contribution of assets to achievement of process goals.

D. determine span of control during life cycle of IT assets.

8. Which of the following is the PRIMARY purpose of optimizing the use of IT resources within an enterprise?

A. To increase likelihood of benefit realization.

B. To ensure readiness for future change.

C. To reduce cost of IT investments.

D. To address dependency on IT capabilities.

9. While monitoring the performance of IT resources the PRIMARY focus of senior management is to ensure that:
   A. IT sourcing strategies focus on using third party services.
   B. IT resource replacements are approved as per IT strategic plan.
   C. key goals and metrics for all IT resources are identified.
   D. resources are allocated in accordance with expected performance.
10. Organization considering deploying application using cloud computing services provided by third party service provider. The MAIN advantage of this arrangement is that it will:
   A. minimize risks associated with IT
   B. help in optimizing resource utilization.
   C. ensure availability of skilled resources.
   D. reduce investment in IT infrastructure.

4.10 Answers and Explanations

1. B. Lead indicators are proactive approach for ensuring performance shall be as expected and hence are defined using industry best practices. Lag indicators are useful after the fact (A), Thresholds based on long term plan may not provide input on performance during execution. (C). All lead indicators may not have lag indicator.
2. C. The Balance score card (BSC) focuses on Financial, Customer, internal and learning perspective.
3. A. Lead indicators are proactive in nature and helps management in planning. Identification of gaps with respect to industry standard is beginning of process of implementing best practices. Other indicators are result of past performance.
4. D. In order to plan resources performance of resource must be determined and compared with business expectation from IT. This will help management in implementing performance measures against expected performance. Other options use baselines.
5. A. Motivation helps human resources in performing better. Career progression planning including in job description along with performance norms shall help in motivating human resources.
6. B. Resource optimization plan primarily focus on availability of right resources at right time. Other requirements are secondary.
7. C. Resource performance is essential to measure the performance of business and IT processes so as to monitor the level of contribution in achieving process goals and hence business objectives. Performance measurement is performed to measure this contribution.

8. A. IT resource optimization within an enterprise must primarily focus on increasing benefit realization from IT so as to deliver value to business. B. Ensuring readiness for future change is essential to meet the growing IT service delivery and is part of resource optimization requirements, but not the primary purpose. C. Resource optimization may or may not reduce IT costs, however it will help in increasing return on IT investment. D. Business dependency on IT depends on capabilities of IT to deliver services to business. Resource optimization is one of the processes to address this dependency not objective.

9. D. Management must monitor the performance of IT resources to ensure that the expected benefits from IT are being realized as per planned performance. This is done by allocating IT resources in accordance to the planned performance of business process cascaded down to IT resources supporting business processes.

10. B. Outsourcing shall help organization in optimizing use of existing IT resources by outsourcing, which in turn shall help in focusing on more critical business requirements and hence improving benefit realization. However, outsourcing may or may not minimize risks associated with IT. i.e. it may minimize risks associated with own investment but may introduce risks associated with outsourcing. Although outsourcing helps in ensuring availability of skilled resources, it is not main advantage. Outsourcing may or may not reduce investment in IT, i.e. it may reduce need for acquisition of IT infrastructure, but there is cost associated with outsourcing and there is additional cost for SLA monitoring.

Chapter 5

Business Continuity Management

Learning Objective

The objective of this chapter is to provide knowledge about the key concepts of Business Continuity Management (BCM), Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Incident Responses, Contingency plan and disaster. It is important to understand these concepts as they form the base and DISA candidate is expected to have understanding of the key terms related concepts as this is critical for designing, implementing or reviewing business continuity. A good understanding and working knowledge in this area will help DISAs to provide assurance and consulting services in this area. This chapter deals with the regulatory requirements that make it mandatory for an organisation to have Business Continuity Management.

5.1 Introduction

A Business Continuity Plan outlines a range of disaster scenarios and the steps the business will take in any particular scenario to return to regular trade. BCP's are written ahead of time and can also include precautions to be put in place. Usually created with the input of key staff as well as stakeholders, a BCP is a set of contingencies to minimize potential harm to businesses during adverse scenarios.

Organisations around the world have been the victims of all sorts of disruptions. Over the years, man-made and natural disasters have unveiled the vulnerability of businesses on a global scale.

Business continuity management (BCM) capabilities enable organisations to restore their businesses to normal operations following an unanticipated disaster or business interruption. The disruption of business operation can be due to unforeseen man-made or natural disaster and this may lead to loss of productivity, revenue and market share among many other impacts. Hence, organisations have to take necessary steps to ensure that the impact from such disasters is minimized and build resilience which ensures continuity of critical operation in the event of disruptions. Modern organisations cannot think of running their business operations without I&T. I&T is prone to increased risks which can lead to failure of I&T thus impacting operations. Hence, it is becoming increasingly important for organisations to have a business contingency plan for their Information Systems.

5.2 Definitions of Key Terms

The concepts of Business Continuity Management are quite simple to understand. However, to understand and implement BCM or BCP as per needs of organisation requirements, it is

knowing the key terms. Knowledge of definition of these terms will help not only in understanding the topics but also to provide assurance, consulting or implementation services in this area.

Business Continuity Planning: Business continuity planning is the process of developing prior arrangements and procedures that enable an organisation to respond to an event in such a manner that critical business functions can continue within planned level of disruption. The end result of the planning is called a Business Continuity Plan.

Crisis: An abnormal situation which threatens the operations, staff, customers or reputation of the organisation.

Disaster: A physical event which interrupts business processes sufficiently to threaten the viability of the organisation.

Emergency Management Team (EMT): This team comprising of executives at all levels including IT is vested with the responsibility of commanding the resources which are required to recover the enterprises operations.

Incident: An event that has the capacity to lead to loss of or a disruption to an organisation's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis or disaster.

Incident Management Plan: A clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process.

Minimum Business Continuity Objective (MBCO): This refers to the minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during an incident, emergency or disaster. As per ISO 22301:2012, clause 3.28, MBCO is the minimum level of services and/or products that is acceptable to the organizations to achieve its business objectives during a disruption. MBCO is used to develop test plan for testing BCP.

Maximum Acceptable Outage (MAO): This is the time frame during which a recovery must become effective before an outage compromises the ability of an Organization to achieve its business objectives and/or survival. This refers to the maximum period of time that an organization can tolerate the disruption of a critical business function, before the achievement of objectives is adversely affected. MAO is also known as maximum tolerable outage (MTO), maximum downtime (MD), Maximum Tolerable Period of Disruption (MTPD).

Recovery Time Objective (RTO): The pre-determined time at which a product, service, or activity must be resumed, or resources must be recovered

Recovery Point Objective (RPO): Maximum data loss, i.e., minimum amount of data used by an activity that needs to be restored

Resilience: The ability of an organisation to resist being affected by the incident.

Risk: The combination of the probability of an event and its consequence.

Vulnerability: The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence.

5.3 Key concepts of Disaster Recovery, Business Continuity Plan and Business Continuity Management

5.3.1 Contingency Plan

An organisation's ability to withstand losses caused by unexpected events depends on proper planning and execution of such plans. Without a workable plan, unexpected events can cause severe damage to information resources and may affect the business continuity. Contingency planning is an overall process of preparing for unexpected events. Its main goal is to restore normal modes of operation with minimal cost and minimal disruption to normal business activities after unexpected event. It should ideally ensure continuous information systems availability despite unexpected events.

5.3.2 Components of Contingency Planning

5.3.2.1 Business Impact Analysis (BIA)

BIA includes tasks like Threat Attack identification and prioritization, Business unit analysis, Attack scenario development, Potential damage assessment, etc. The steps involved in impact analysis are risk evaluation, defining critical functions in the organisation, identifying critical facilities required for providing recovery of the critical functions and their interdependencies and finally setting priorities for all critical business applications which need to be recovered within defined timelines.

5.3.2.2 Incident Response Plan (IR plan)

IR Plan includes tasks like incident planning, incident detection, incident reaction, incident recovery etc. Incident Response plan gives an entity a set of procedures and guidelines that is needed by an entity to handle an incident.

5.3.2.3 Business Continuity Plan (BCP)

BC Plan includes tasks like establishing continuity strategies, planning for continuity of critical operations, continuity management etc. Business Continuity Plan is a plan that contains the steps that would be taken by an entity to resume its business functions during its period of disruption. These plans are executed in parallel with the disaster recovery plans depending on the impact of the disaster. Business Continuity Plans on a whole is about re-establishing existing business processes and functions, communications with the business contacts and resuming business processes at the primary business location.

5.3.2.4 Disaster Recovery Plan (DRP)

DR Plan includes tasks like plan for disaster recovery, crisis management, recovery operations etc. Disaster Recovery Plan is the set of plans which are to be executed initially at the moment of crisis. These plans include measures to control the disaster, mitigate them and to initiate the recovery of the resources that is needed for the continuity of business. These plans are targeted to initiate/recover the resources that have been affected by a disaster. These are the first plans that would be executed at the time of disaster.

There are three basic strategies that encompass a disaster recovery plan: preventive measures, detective measures, and corrective measures. Preventive measures will try to prevent a disaster from occurring. These measures seek to identify and reduce risks. They are designed to mitigate or prevent an event from turning into a disaster. These measures may include keeping data backed up and off site, using surge protectors, installing generators and conducting routine inspections. Detective measures are taken to discover the presence of any unwanted events within the I&T infrastructure. Their aim is to uncover new potential threats. They may detect or uncover unwanted events. These measures include installing fire alarms, using up-to-date antivirus software, holding employee training sessions, and installing server and network monitoring software. Corrective measures are aimed to restore a system after a disaster or otherwise unwanted event takes place. These measures focus on fixing or restoring the systems after a disaster and may include keeping critical documents in the DRP or securing proper insurance policies.

5.3.3 Business Continuity Plan vs. Disaster Recovery Plan

The primary objective of Business Continuity Plan is to ensure that mission critical functions and operations are recovered and made operational in an acceptable time frame. A BCP aims to sustain critical business process during an unplanned interruption period and a DRP is to re-establish the primary site into operation with respect to all business processes of the organisation facing the disaster.

5.3.4 Business Continuity Management

BCM is a holistic process that identifies potential threats and the impacts on normal business operations should those threats actualize. BCM provides a framework to develop and build the organisation's resilience with the capability for an effective response, therefore ensuring that critical objectives are met, safeguarding key stakeholder’s interests and the organisation's reputation, brand and value creating activities. The purpose of BCM is to minimize the operational, financial, legal, reputational and other material consequences arising from a disruption due to an undesired event (Basel Committee on Banking Supervision, 2005), minimizing losses and restoring normal, regular operations in the shortest, possible time. Coupled with security measures to protect the organisation's assets, BCM requires plans and strategies that should cater for and allow responses, contingency plans and procedures to

recover as quickly as possible. BCM looks at an entirety of the businesses of the entity as a whole. It is a continuous process whereby risks which are inherent to the business are closely monitored and mitigated.

Figure 5.1: BCP / DRP

5.4 Objectives of BCP and BCM

5.4.1 Objectives of Business Continuity Plan

The primary objective of a Business Continuity Plan (BCP) is to enable an organisation to continue to operate through an extended loss of any of its business premises or functions.

The key objectives of BCP are:

- Manage the risks which could lead to disastrous events.
- Reduce the time taken to recover when an incident occurs and

- Minimize the risks involved in the recovery process.
- Reduce the costs involved in reviving the business from the incident.

5.4.2 Objectives of Business Continuity Management (BCM)

The objective of BCM is to counteract interruptions to business activities and to protect critical business processes from the impact of major failures or disasters. The detailed objectives of BCM are:

- Reduce likelihood of a disruption occurring that affects the business through a risk management process.
- Enhance organisation's ability to recover following a disruption to normal operating conditions.
- Minimize the impact of that disruption, should it occur.
- Protect staff and their welfare and ensure staff knows their roles and responsibilities.
- Tackle potential failures within organisation's I.S. Environment
- Protect the business.
- Preserve and maintain relationships with customers.
- Mitigate negative publicity.
- Safeguard organisation's market share and/or competitive advantage.
- Protect organisation's profits or revenue and avoid financial losses.
- Prevent or reduce damage to the organisation's reputation and image.

5.4.2.1 Need for BCM at Business Level

The need for BCM arises because of the following present-day requirements of business

- Need to provide access to potentially millions of new customers.
- Need to ensure security, privacy and confidentiality.
- Need to integrate business processes onto web.
- Need to integrate business partners into key business processes.
- Increased pressure on delivering quality customer service 24x7.
- Emerging pervasive computer devices.

Business and organisations of today depend heavily on Information and Communication Technology (ICT) to conduct business. The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. This dependence on the systems means that all organisations should have

contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen manmade or natural disaster that may result into revenue loss, productivity loss and loss of market share among many other impacts. Thus, organisations have to take necessary steps to ensure continuity of operation in the event of disruptions. Business continuity is the activity performed by an organisation to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

5.4.2.2 Need for BCM at Various Levels of I&T Environment

Disaster Recovery is an essential phase to critical I&T Resources. I&T Infrastructure generally includes Servers, Workstations, Network and Communication, Operating system software, business applications software, essential utility software, Data Centres, Support Desks, IT Personnel, Disks, Tapes etc. In this technologically driven world, I&T Infrastructure has essentially become an integral part of an entity's anatomy. Mail Servers and communication lines like Internet, Phone and Fax are also essentially the important components of the Infrastructure. It is therefore critical to get these components up and running for a successful recovery of the business. Therefore, when critical industries like Banks, Insurance Companies, Stock Exchanges, Airline Companies, Railways, Multinational Companies, Government Agencies rely on I&T Infrastructure for its daily operations, it is crucial to maintain BCM for such organisations. Software like the Core Banking Systems, SWIFT Financial Messaging Services, Airline Communication Services like AMADEUS, Stock Market Trading Applications, ERP Systems, e-commerce sites and many more are critical where no downtime is tolerated. These applications are used to conduct transactions worldwide and are run only on extensive I&T Resources. BCM therefore is a much-needed requirement for a quick recovery from a crisis to ensure survival of the business.

Figure 5.2: Contingency Plan

5.5 Various Types of Disaster

BCM or BCP is all about planning in advance to meet future unforeseen events which may impact or disrupt business operations. Disasters are the major source of disruptions. As distinguished from an event which causes disruption for a short period of time and addressed through incident management plan, disaster is of various types and can have varying and serious impact. This section will provide an overview of various types of disasters.

A disaster can be defined as an unplanned interruption of normal business process. It can be said as a disruption of business operations that stops an organisation from providing critical services caused by the absence of critical resources. An occurrence of disaster cannot always be foreseen; hence we need to be prepared for all the types of disasters that can arise, handle them effectively in the shortest time.

A disaster can be natural or man-made (or technological) hazard resulting in an event of substantial extent causing significant physical damage or destruction, loss of life, or drastic change to the environment. A disaster can be defined as any tragic event stemming from events such as earthquakes, floods, catastrophic accidents, fires, or explosions. It can cause damage to life and property and destroy the economic, social and cultural life of people. For a clear~~er~~ understanding of the concept of disasters, disasters can be classified into two major categories as:

1. Natural disasters
2. Man-made disasters

1. Natural Disasters

Natural Disasters are those which are a result of natural environment factors. A natural disaster has its impact on the business's that is present in a geographical area where the natural disaster has struck. Natural disasters are caused by natural events and include fire, earthquake, tsunami, typhoon, floods, tornado, lightning, blizzards, freezing temperatures, heavy snowfall, pandemic, severe hailstorms, volcano etc.

2. Man-Made Disasters

Man-made disasters are artificial disasters which arise due to the actions of human beings. Artificial disasters has its impact on a business entity specific to which it has occurred. Artificial disasters arising due to human beings Include Terrorist Attack, Bomb Threat, Chemical Spills, Civil Disturbance, Electrical Failure, Fire, HVAC Failure, Water Leaks, Water Stoppage, Strikes, Hacker attacks, Viruses, Human Error, Loss Of Telecommunications, Data Centre outrage, lost data, Corrupted data, Loss of Network services, Power failure, Prolonged equipment outage, UPS loss, generator loss and anything that diminishes or destroys normal data processing capabilities.

5.6 Phases of Disaster

It is important to envisage what is the impact when a disaster strikes and decide in advance the action to be taken for various types of disaster scenarios. A typical disaster will consist of some or all of the following phases:

1. Crisis phase
2. Emergency response phase
3. Recovery phase
4. Restoration phase

1. Crisis Phase

The Crisis Phase is under the overall responsibility of the Incident Control Team (ICT). It comprises the first few hours after a disruptive event starts or the threat of such an event is first identified; and is caused by, for example:

- Ongoing physical damage to premises which may be life threatening, such as a fire; or
- Restricted access to premises, such as a police cordon after a bomb incident. During the crisis phase, the fire and other emergency evacuation procedures (including bomb threat and valuable object removal procedures) will apply; and the emergency services should be summoned as appropriate.

2. Emergency Response Phase

The Emergency Response Phase may last from a few minutes to a few hours after the disaster. It will start near the end of, or after, the crisis Phase if there has been one, or when a potentially threatening situation is identified. During the Emergency Response Phase, the Business Continuity Team (BCT) will assess the situation; and decide if and when to activate the BCP.

3. Recovery Phase

The Recovery Phase may last from a few days to several months after a disaster and ends when normal operations can restart in the affected premises or replacement premises, if appropriate. During the recovery phase, essential operations will be restarted (this could be at temporary premises) by one or more recovery teams using the BCP; and the essential operations will continue in their recovery format until normal conditions are resumed.

4. Restoration Phase

This phase restores conditions to normal. It will start with a damage assessment, usually within a day or so of the disaster, when the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the restoration phase, any damage to the premises and facilities will be repaired.

5.7 Examples of Disaster

Some examples of disasters and the phases that may impact disaster phases of a business continuity plan are:

Serious fire during working Hours	All phases in full
Serious fire outside during working hours	All the phases, however, no staff and public evacuation
Very minor fire during working hours	Crisis Phase only, staff and public evacuation but perhaps no removal of valuable objects, Fire Service Summoned to deal with the fire
Gas leak outside or during working hours, repaired after some hours	Only emergency response phase is appropriate

5.8 Impact of Disaster

The impact of a disaster can varies and could result in:

- Total destruction of the premises and its contents. For example, as a result of a terrorist attack;
- Partial damage, preventing use of the premises. For example, through flooding; or
- No actual physical damage to the premises but restricted access for a limited period, such as enforced evacuation due to the discovery nearby of an unexploded bomb.

The impact of a disaster may result in one or more of the following:

(i) Loss of Human Life: The extent of loss depends on the type and severity of the disaster. Protection of human life is of utmost importance and, the overriding principle behind continuity plans.

(ii) Loss of productivity: When a system failure occurs, employees may be handicapped in performing their functions. This could result in productivity loss for the organisation.

(iii) Loss of revenue: For many organisations like banks, airlines, railways, stock brokers, effect of even a relatively short breakdown may lead to huge revenue losses.

(iv) Loss of market share: In a competitive market, inability to provide services in time may cause loss of market share. For example, a prolonged non-availability of services from services providers, such as Telecom Company or Internet Service Providers, will cause customers to change to different service providers.

(v) Loss of goodwill and customer services: In case of a prolonged or frequent service disruption, customers may lose confidence resulting in loss of faith and goodwill.

(vi) Litigation: Laws, regulations, contractual obligation in form of service level agreement govern the business operations. Failure in such compliance may lead the company to legal litigations and lawsuits.

When considering the impact of a disaster, it should be remembered that it will never happen at a convenient time; and is always unpredictable. There is no way of knowing:

- When it will happen;
- What form it will take;
- How much damage it will cause; or
- How big the impact will be?

However, it is important to envisage various types of scenarios to ensure that the coverage is as comprehensive as feasible covering various types of events with varying impact. Understanding disaster and their impact is the key to successful business impact analysis which will result to preparation of an effective business continuity plan.

5.9 Invoking a DR Phase / BCP Phase

5.9.1 Operating Teams of Contingency Planning

Contingency Planning Team: This team collects data about information systems and threats, conducts business impact analysis, and creates contingency plans for incident response, disaster recovery, business continuity. The primary role of this team is to conduct research on data that could lead to a crisis and develop actions that would effectively handle these threats.

Incident Response Team: This team manages/executes IR plan by detecting, evaluating, responding to incidents. This team is the first team to arrive during the outbreak of an incident. Incident Response Team evaluates the incident, takes the first action to stop the incident. If unsuccessful, then summons the Disaster Recovery Team.

Disaster Recovery Team: This team manages/executes DR plan by detecting, evaluating, responding to disasters; re-establishes primary site operations. This team plays its role in reducing the impact of the disaster and executes the steps that are defined in the DR Plan to recover and protect resources that are being impacted by the disaster and to mitigate the disaster itself. If the impact of the crisis is very high, then the Business Continuity Team steps in parallel to the DR Team and

Business Continuity Team: This team manages/executes BC plan by establishing off-site operations to ensure Business Continuity. Business Continuity Team initiates those responses to the impacts that are being faced by the entity and would bring the entity back to its original level of business functioning. The disaster recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information Technology Services Locations. Each supported application or platform has a

section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organisational structure for the recovery process. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, the plan should be treated as a confidential document and should be shared with specific employees as per the specific responsibilities they have been assigned.

5.10 Disaster Recovery Plan (DRP) Scope and Objectives

The DRP should inform the user about the primary focus of this document like responding to disaster, restoring operations as quickly as possible and reducing the number of decisions which must be made when, and if, a disaster occurs. It should also inform about the responsibility to keep this document current. It should be approved by appropriate authority.

The overall objectives of this plan are to protect organisation's computing resources and employees, to safeguard the vital records of which Information Technology Systems and to guarantee the continued availability of essential Information Technology services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data centre and its services.

This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as a part of the total plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the plan is organized around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current I&T and business environment. The IS Auditor has to review the process followed for preparation of the DRP and assess whether it meets the requirements of the organisation and provide recommendations on any areas of weaknesses identified.

5.11 Disaster Recovery Phases

The disaster recovery process consists of four phases which are outlined here:

- Phase 1: Disaster Assessment
- Phase 2: Disaster Recovery Activation
- Phase 3: Alternate Site/Data Centre Rebuild
- Phase 4: Return to Primary site

1. Disaster Assessment: The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Cooperation with emergency services personnel is critical.
2. Disaster recovery activation: When the decision is made to move primary processing to another location, this phase begins. The Disaster Recovery Management Team will assemble and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.
3. Alternate site operation/data centre rebuild: This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.
4. Return to primary site: This phase involves the reactivation of the primary site at either the original or possibly a new location. The activation of this site does not have to be as rushed as the activation of the alternate recovery site. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

5.12 Key Disaster Recovery Activities

The declaring of an incident/event is done by assigned personnel of management. Declaration of a disaster means:

1. Activating the recovery plan
2. Notifying team leaders
3. Notifying key management contacts
4. Redirecting information technology service to an alternate location
5. Securing a new location for the data centre
6. Ordering and configuring replacement equipment
7. Reconfiguring the network
8. Reinstalling software and data
9. Keeping management informed

10. Keeping users informed
11. Keeping the public informed

5.12.1 DRP

The DRP should contain information about the vital records details including location where it is stored, who is in charge of that record etc. It contains information about what is stored offsite such as:

1. A current copy of this disaster recovery plan.
2. Copies of install disks for all relevant software and critical software/operating system licenses. These should be stored electronically rather than relying on Internet-downloadable versions. When the software is needed the same version of the software used may not be available on the Internet, or there may be Internet issues that could negatively affect large downloads or may significantly slow down the recovery process.

5.12.2 Disaster Recovery Team

The disaster recovery plan should contain details about Disaster Recovery Management Team and its sub-teams like Administration, Supplies, Public relations etc. and their respective responsibilities. The various types of responsibilities applicable in case of a disaster are explained here covering specific stages.

5.12.2.1 General Responsibilities

The IT Disaster Recovery Management Team is responsible for the overall coordination of the disaster recovery process from an Information Technology Systems perspective. The other team leaders report to this team during a disaster. In addition to their management activities, members of this team will have administrative, supply, transportation, and public relations responsibilities during a disaster. Each of these responsibilities should be headed by a member of the IT Disaster Recovery Management Team.

5.12.2.2 General Activities

- Assess the damage and if necessary, declare a disaster (damage assessment forms are included in this plan)
- Coordinate efforts of all teams
- Secure financial backing for the recovery effort
- Approve all actions that were not pre-planned
- Give strategic direction
- Be the liaison to upper management
- Expedite matters through all bureaucracy
- Provide counselling to those employees that request or require it

- After the Disaster Make recommendations on how the disaster recovery plan can be improved

5.12.2.3 *Administrative* Responsibilities

The administrative function provides administrative support services to any team requiring this support. This includes the hiring of temporary help or the reassignment of other clerical personnel.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Notify all vendors and delivery services of change of address

Procedures during All Phases

- Process expense reports
- Account for the recovery costs
- Handle personnel problems

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.4 Supply Responsibilities

The supply function is responsible for coordinating the purchase of all needed supplies during the disaster recovery period. Supplies include all computing equipment and supplies, office supplies such as paper and pencils, and office furnishings.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Purchase supplies required by the teams at the alternate site.

Procedures during Remote Operation/Data Centre Rebuild Phase

- Work with procurement to order replacement supplies and expedite shipments
- Ongoing distribution of supplies

Procedures during return to primary site Phase

- Restock supplies at the restored site

After the disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.5 Public Relations Responsibilities

The public relations function will pass appropriate information about the disaster and associated recovery process to the public and to employees. Every effort should be made to

give these groups reason to believe that the organization is doing everything possible to minimize losses and to ensure a quick return to normalcy.

Activities by Phase

All Phases

- Ensure that employees do not talk to the media
- Control information released to the public and to employees
- Interface with organisation's Public Relations or defer to Senior Management
- Publish internal newsletters
- Keep everyone aware of recovery progress

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Management Team Call Checklist

The disaster recovery plan should contain disaster recovery management team call checklist. It should specify the contact information about Team leader as well as team members with the details on which functionality he/she can be contacted. The disaster recovery plan should contain details about Technical support Team and its sub-teams like Hardware, Software, Network, Operations etc. and their respective responsibilities.

5.12.2.6 Hardware Responsibilities

The responsibility of the Hardware Team is to acquire (along with the Facilities Team), configure and install servers and workstations for organisational information Technology users.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Determine scope of damage for servers and workstations
- Order appropriate equipment and supplies (coordinate and work with the Facilities Team for this activity)

Procedures during Remote Operation/Data Centre Rebuild Phase

- Set up servers and workstations
- Install software as necessary
- Restore data
- Install additional workstations as they arrive

Procedures during Return Home Phase

- Notify users
- Ensure data is backed up
- Relocate equipment

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.7 Software Responsibilities

The responsibility of the Software Team is to maintain the systems software at the alternate site and reconstruct the system software upon returning to the primary site. In addition, the Software Team will provide technical support to the other teams.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

Procedures during Remote Operation/Data Centre Rebuild Phase

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

Procedures during Return Home Phase

- Provide technical support to the other teams
- Verify that the system is performing as expected

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.8 Network Responsibilities

The Network Team is responsible for preparing for voice and data communications to the alternate location data centre and restoring voice and data communications at the primary site.

Activities by Phase

Procedures during disaster recovery activation phase

- Determine the requirements for voice and data communications
- Install the network including lines, routers, switches, controllers and other communications equipment at the alternate location data centre
- Test the network.

Procedures during Remote Operation/Data Centre Rebuild Phase

- Operate the backup network
- When the replacement equipment arrives at the primary site, install it

Procedures during Relocation Home Phase

- Support the primary site network
- Dismantle the alternate location data centre network

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.9 Operations Responsibilities

The Operations responsibilities include the daily operation of computer services and management of all backup tapes. When a disaster is declared, the team must secure the correct tapes for transport to the alternate location. Once operations are established at the alternate location, arrangements must be made with an offsite storage service.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Inventory and select the correct backup tapes
- Transport the tapes to the alternate data centre
- Assist all teams in restoring the production environment at the alternate data centre

Procedures during Remote Operation/Data Centre Rebuild Phase

- Establish a production schedule at the alternate location
- Run the daily schedule at the alternate location
- Perform system and production backups at the alternate location

- Assist other teams in preparing the primary site
- Establish offsite storage at the alternate location

Procedures during Return Home Phase

- Perform system and production backups
- Inventory all tapes at the alternate data centre
- Transport all tapes from the alternate data centre to the primary site

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Technical Support Team Call Checklist

The disaster recovery plan should contain Disaster Recovery Technical Support Team Call Checklist. It should specify the contact information about Team leader as well as team members with the details on which functionality he/she can be contacted. The disaster recovery plan should contain details about Facility Team and its sub-teams like Salvage team, new data centre, new hardware team etc. and their respective responsibilities.

5.12.2.10 Salvage Responsibilities

The Salvage Team is responsible for minimizing the damage at the primary site and to work with the insurance company for settlement of all claims. This depends on a quick determination of what equipment is salvageable and what is not. Repair and replacement orders will be filed for what is not in working condition. This team is also responsible for securing the disaster recovery data centre.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Establish the command centre
- Assist in the immediate salvage operations
- Contact Insurance representatives
- Inventory all equipment in the data centre. If necessary, involve the vendors.

Procedures during Remote Operation/Data Centre Rebuild Phase

- Salvage equipment and supplies
- Settle property claims with the insurance company
- Provide for security at the data centre

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.11 New Data Centre Responsibilities

The New Data Centre Team is responsible for locating the proper location for a new data centre and overseeing the construction of it. This includes the environmental and security controls for the room.

Activities by Phase

Procedures during Remote Operation/Data Centre Rebuild Phase

- Determine the requirements for a new data centre
- Work with contractors and university staff on the details
- Oversee the construction of the new data centre

Procedures during Return Home Phase

- Ensure that all controls are working as designed

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

5.12.2.12 New Hardware Responsibilities

The New Hardware Team is responsible for ordering replacement hardware for equipment damaged in the disaster and installing it in the new or rebuilt data centre. Depending on the age of the damaged hardware, replacement may not be one-for-one. All types of hardware are to be handled, including:

1. Servers
2. Printers
3. Switches, Routers, Hubs
4. Work stations
5. Environmental systems
6. UPS Equipment

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Obtain a list of damaged and destroyed equipment

Procedures during Remote Operation/Data Centre Rebuild Phase

- Determine what new hardware should be ordered
- Order new hardware

- Arrange for installation and testing of the new hardware

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Resumption of Normal Operations

Once the threat has passed, equipment has been repaired or replaced or a new primary site has been built and stocked, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations

5.13 Documentation: BCP Manual and BCM Policy

All documents that form the BCM are to be subject to document control and record control processes. The following documents (representative only) are classified as being part of the business continuity management system:

- The business continuity policy;
- The business continuity management system;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- SLA with alternate site/mirror site with switchover plans
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training Program

To provide evidence of the effective operation of the BCM, records demonstrating the operation should be retained as per policy of the organisation and as per applicable laws, if any. These records also include reference to all business interruptions and incidents, irrespective of the nature and length of disruption. This also includes general and detailed definition of requirements as described in developing a BCP. In this, a profile is developed by

identifying resources required to support critical functions, which include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit.

5.13.1 BCM Policy

While developing the BCM policy, the organisation should consider defining the scope, BCM principles, guidelines and applicable standards for the organisation. They should consider all relevant standards, regulations and policies that have to be included or can be used as benchmark. The objective of this policy is to provide a structure through which:

- Critical services and activities undertaken by the organisation will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans and BCP are subject to ongoing testing, revision and updating as required.
- Planning and management responsibility are assigned to members of the relevant senior management team.

The BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability. The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability. The ongoing maintenance and management activities include embedding business continuity within the organisation, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process, market, technology or organisational structure.

5.13.2 BCP Manual

An incident or disaster affecting critical business operations can strike at any time. Successful organisations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. A BCP manual consists of the Business Continuity Plan and the Disaster Recovery Plan. The primary objective of preparing BCP manual is to provide reasonable assurance to senior management of organisation about the capability of the organisation to recover from any unexpected incident or disaster affecting business operations and continue to provide services with

minimal impact. Further, the BCP should be comprehensive and anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services. The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of organisation's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as visioning teams between the functional area(s) affected and other departments providing support services.

5.13.2.1 Elements of BCP Manual

The plan will contain the following elements:

1. Purpose of the plan: Included in this section should be a summary description of the purpose of the manual. It should be made clear that the manual does not address recovery from day to day operational problems. Similarly, it must be stressed that the manual does not attempt to foresee all possible disasters, but rather provides a framework within which management can base recovery from any given disaster.

2. Organisation of the manual: A brief description of the organisation of the manual, and the contents of each of the major sections, will provide the reader with the direction to the relevant section of the manual in an emergency situation. Any information which is external to the manual but will be required in an emergency should be identified in this section.

3. Disaster definitions: It may assist the user of the manual if a definition of disaster classification is provided, together with an identification of the relevance of the plan to that situation. Four types of classification can generally be used:

- Problem/Incident: Event or disruptions that cause no significant damage.
- Minor disaster: Event or disruption that causes limited financial impact,
- Major disaster: Event or disruptions that cause significant impact and may have an effect on outside clients.
- Catastrophic disaster: Event or disruption that has significant impact and adversely affect the organisation's "going concern" status

The BCP manual of each organisation is expected to classify disasters, after taking into account the size and nature of its business and the time and cost associated to each kind of disaster should be defined as per the requirement of the individual organisation. It should be noted, however, that development of a plan based on each classification is not recommended. The need to invoke the plan should be determined by the length and associated cost of the expected outage and not the classification of the disaster, although there is a direct correlation. These definitions will be most useful for communication with senior management.

4. Objectives of the plan: The objectives of the manual should be clearly stated in the introductory section. Typically, such objectives include:

- Safety/security all personnel. The paramount objective of a BCP is to ensure the safety and security of people (both employees and others who may be affected in the event of a disaster). The safeguarding of assets/data is always a secondary objective.
- the reduction of confusion in an emergency
- the identification of critical application systems and / or business functions
- the identification of all resources, including personnel, required to recover the critical business functions
- the identification of alternative means of ensuring that the critical business functions are performed and
- The establishment of a workable plan to recover the critical business functions, and subsequently resume normal operations, as quickly as possible after a disaster.

The list should be expanded as necessary to meet the requirements of any given plan.

5. Scope of the plan: In order that there is no confusion as the situations in which the plan will apply, the scope of the plan must be clearly identified. Any limitations must be explained.

6. Plan approach / recovery strategy: A step by step summary of the approach adopted by the plan should be presented. For ease of reference, it may be good to provide this overview by means of a schematic diagram. In particular, it may be useful to set up the recovery process as a project plan in this section.

7. Plan administration: The introductory section should also identify the person or persons, responsible for the business continuity plan manual, and the expected plan review cycles. These persons will be responsible for issuing revisions which will ensure that the plan remains current. Because the manual will include staff assignments, it is also advisable that the personnel or human resource function accept responsibility for notifying the plan administrators of all personnel changes which must be reflected in the plan.

8. Plan management: Following a disaster, the normal reporting channels and lines of management are unlikely to be strictly adhered to. During a disaster, reporting by exception may be the only feasible way to operate. This does not however negate the requirement for formalized management. The management responsibilities and reporting channels to be observed, during disaster recovery should be clearly established in advance.

9. Disaster notification and plan activation procedures: The procedures represent the first steps to be followed when any disaster occurs. It is recommended that the procedures be written in a task-oriented manner and provide a logical flow to enable ease of management.

5.14 Data backup, Retention and Restoration Practices

5.14.1 Back up Strategies

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are:

- Dual recording of data: Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- Periodic dumping of data: This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.
- Logging input transactions: This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded, and reprocessing of the transactions are carried out which were logged since the last dump.
- Logging changes to the data: This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

Apart from database backup strategies as mentioned above, it is important to implement email and personal files backup policies. The policy can be like burning DVDs with the folders and documents of importance periodically to more detailed and automated functions. The choice depends and varies with the size, nature and complexity of the situation. For example, individuals are responsible for taking backups of personal files and folders. However, a policy may be there whereby individual users may transfer personal files and folders from the PC to an allocated server space. The data so transferred in the server will be backed up by the IT department as a part of their routine backup. Email backups should necessarily include the address book backup. However, the most important and critical part of the backup strategy is to include a restoration policy. Restoration of the data from the backup media and devices will ensure that the data can be restored in time of emergency; else a failed backup is a double disaster. The restoration should be done for all backups at least twice a year.

5.14.2 Types of Backup

When the back-ups are taken of the system and data together, they are called total system's back-up. An organisation has to choose the right type of back up for each of the critical components of IS and data to meet specific business requirements. The various types of back-ups are:

- Full Backup: A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the

backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

- Incremental Backup: An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, incremental backup is very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- Differential Backup: A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved. Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.
- Mirror Backup: A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. Mirror backup is most frequently used to create an exact copy of the backup data.

5.14.3 Recovery Strategies

The backup plan is intended to restore operations quickly so that information system function can continue to service an organisation, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery team that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the various departments and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of the recovery team must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If employees leave the organisation, new employees must be assigned the responsibility immediately and briefed about their responsibilities. The recovery strategies for various types of information systems are outlined here.

5.14.4 Strategies for Networked Systems

Most organisations use networked systems. There is heavy dependence on main server and network in case of networked systems. The recovery strategy would vary depending on the type of network architecture and implementation. For example, LANs can be implemented in two main architectures:

5.14.4.1 LAN Systems

Peer-to-Peer: Each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a hub to share data.

Client/Server: Each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources. A LAN's topology, protocol, architecture, and nodes will vary depending on the organisation. Thus, contingency solutions for each organisation will be different. Listed below are some of the strategies for recovery of LANs.

1. Eliminating Single Points of Failure (SPOC): When developing the LAN contingency plan, the organisation should identify single points of failure that affect critical systems or processes outlined in the Risk Assessment. These single points of failures are to be eliminated by providing alternative or redundant equipment.

2. Redundant Cabling and Devices: Contingency planning should also cover threats to the cabling system, such as cable cuts, electromagnetic and radiofrequency interference, and damage resulting from fire, water, and other hazards. As a solution, redundant cables may be installed when appropriate. For example, it might not be cost-effective to install duplicate cables to every desktop. However, it might be cost-effective to install a redundant cable between floors so that hosts on both floors could be reconnected if the primary cable were cut. Contingency planning also should consider network connecting devices such as hubs, switches, bridges, and routers.

3. Remote Access: Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working off-site or allows for a means for servers and devices to communicate between sites.

Remote access can be conducted through various methods, including dialup access and virtual private network (VPN). Remote access may serve as allocation that can access the corporate data even when they are not in a position to reach the physical premises due to some calamity. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented, if the communication traffic contains sensitive information.

5.14.4.2 Wireless LANs

Wireless local area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing wireless network, security controls, such as data encryption, should be implemented, if the sensitive information is to be communicated.

5.14.5 Strategies for Distributed Systems

A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server model to make the application more accessible to users in different locations. Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system (DBMS) that supports organisation wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each location, and users access the system from their local server. The contingency strategies for distributed system reflect the system's reliance Nolan and WAN availability. Based on this fact, when developing a distributed system contingency strategy, the following methods applicable to system backups should be considered for decentralized systems. In addition, a distributed system should consider WAN communication link redundancy and possibility of using Service Bureaus and Application Service Providers (ASPs).

5.14.6 Strategies for Data Communications

(i) Dial-up: Using Dial-up as a backup to normal leased or broadband communications lines remains the most popular means of backing up wide-area network communications in an emergency. This approach requires compatible modems at each remote site and at the recovery location. Ideally, the modems should be full duplex modems which will permit transmission and receipt down the same line. The half-duplex option will require two telephone lines for each data line lost.

(ii) Circuit extension: Circuit extension techniques are usually applied to high bandwidth communications services, such as high speed leased lines. This technique builds redundancy into the client's network, by including the recovery site as a defined and serviced node. This is by, where the communications from the remote sites can be directed to the primary site or the recovery site from the carrier's central office. This is effective duplication of equipment and facilities, but with some potential for sharing the costs of the equipment at the recovery site.

(iii) On-demand service from the carriers: Many carriers now offer on-demand services which provide the mechanisms to switch communications to the recovery site from the primary site on client notification.

(iv) Diversification of services: The use of diverse services provides the best solutions to the loss of a carrier central office. Diversity can be achieved in a number of manners, including: Use of more than one carrier on a regular basis. If the organisation uses two or more carriers, it will likely pay above the odds for its regular service and require investment in

some additional equipment. For this approach to communications recovery to work, there must also be some redundancy accommodated following any carrier outage.

(v) Microwave communications: The regular communications can be backed up by the use of microwave communications. This could be used to: backup communications from the central office to the primary site, in case of breakage in the land lines; backup communications from the central office to the recovery centre; or a backup link from a company-controlled communications centre direct to the recovery centre.

(vi) VSAT (Very Small Aperture Terminal) based satellite communications: Companies are increasingly looking to VSAT communications as a cost-effective means of communicating large volumes of information. This technique could similarly be used to back up the primary carrier service. The use of this technology requires VSAT terminals to be installed at each remote location and at the recovery centre if it does not currently provide such a service.

5.14.7 Strategies for Voice Communications

Many of the techniques and concerns above relate to voice communications as wells data, and this will continue with the expansion of ISDN services for integrated voice and data communications. Other techniques available for voice recovery include:

(i) Cellular phone backup: If the regular voice system is inoperative, key employees can be provided with cellular phones as a backup. Given that cellular phones are not run by the major carriers from the same central offices, this also provides coverage for the loss of the central office. Such phones could also be used on an on-going basis and could be used to balance the load on the main PBX switch. Cellular services can also be extended to data and facsimile transmission.

(ii) Carrier call rerouting systems: Most of the major carriers now provide customers with call rerouting services such that all calls to a given number can be rerouted to another number temporarily. While this will not be possible in the case of a carrier outage, it can be used for the rerouting of critical business communications following a disaster at a client's offices. Calls can be rerouted to call management service, for example, to support the client in the interim.

5.15 Types of Recovery and Alternative Sites

The traditional focus of BCP/DRP was the recovery of the corporate computer system, which was almost always a mainframe or large minicomputer. Mainframe centric disaster recovery plans often concentrated on replacing an inaccessible or non-functional mainframe with compatible hardware. A backup site or work area recovery (alternate processing site) site is a location where an entity can easily function out of immediately following a disaster. This is an integral part of a DRP or BCP. Types of alternate processing sites are outlined along with some of the widely adopted strategies for centralized system recovery.

5.15.1 Mirror Site/ Active Recovery Site

5.15.1.1 Mirror Site

The single most reliable system backup strategy is to have fully redundant systems called an active recovery or mirror site. While most companies cannot afford to build and equip two identical datacentres, those companies that can afford to do so have the ability to recover from almost any disaster. This is the most reliable and also the most expensive method of systems recovery.

5.15.1.2 Hot Site

A dedicated contingency centre, or 'hot site' is a fully equipped computer facility with electrical power, heating, ventilation and air conditioning (HVAC) available for use in the event of a subscriber's computer outage. These facilities are available to a large number of subscribers on a membership basis and use of site is on a 'first come, first served' basis. In addition to the computer facility, these facilities offer an area of general office space and computer ready floor space on which the users can build their own long-term recovery configuration. Some of the vendors also offer remote operations facilities for use in tests or emergency. Where the recovery centre is in a city other than the subscriber's home location, this can be used to reduce the need to transport staff and resources.

A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organisations that operate real time processes such as financial institutions, government agencies and ecommerce providers.

5.15.1.3 Cold Site

A cold site is the least expensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

5.15.1.4 Warm Site

A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or

even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

5.15.1.5 Near Site

A near site is a backup storage location in close proximity to the primary processing location that provides easy access to the data

5.15.2 Offsite Data Protection

Offsite data protection is the strategy of sending critical data out of the main location as a part of DRP. Data is usually transported off-site using removable storage media such as magnetic tape or optical storage. Data can also be sent electronically via a remote backup service, which is known as electronic vaulting or e-vaulting. Sending backups off-site ensures systems and servers can be reloaded with the latest data in the event of a disaster, accidental error, or system crash. Sending backups off-site also ensures that there is a copy of pertinent data that isn't stored on-site. Off-site backup services are convenient for companies that backup pertinent data on a daily basis. The different types of Offsite Data Protection are outlined here.

5.15.2.1 Data Vaults

Backups are stored in purpose-built vaults. There are no generally recognized standards for the type of structure which constitutes a vault. Commercial vaults fit into three categories:

1. Underground vaults
2. Free-standing dedicated vaults
3. Insulated chambers sharing facilities

5.15.2.2 Hybrid Onsite and Offsite Vaulting

Hybrid on-site and off-site data vaulting, sometimes known as Hybrid Online Backup, involve a combination of Local backup for fast backup and restore, along with Off-site backup for protection against local disasters. This ensures that the most recent data is available locally in the event of need for recovery, while archived data that is needed much less often is stored in the cloud. Hybrid Online Backup works by storing data to local disk so that the backup can be captured at high speed, and then either the backup software or a D2D2C (Disk to Disk to Cloud) appliance encrypts and transmits data to a service provider. Recent backups are retained locally, to speed data recovery operations. There are a number of cloud storage appliances on the market that can be used as a backup target, including appliances from CTERA Networks, Naquin, StorSimple and Twin Strata.

Aternate Site Selection Criteria					
SITE	COST	HARDWARE EQUIPMENT	TELECOMM UNICATIONS	SET UP TIME	LOCATION
COLD SITE	Low	None	None	Long	Fixed
WARM SITE	Medium	Partial	Partial/ Full	Medium	Fixed
HOT SITE	Medium/ High	Full	Full	Short	Fixed
MOBILE SITE	High	Dependent	Dependent	Dependent	Not Fixed
MIRRORED SITE	High	Full	Full	None	Fixed

Figure 5.3: Site Selection Criteria

5.16 System Resiliency Tools and Techniques

5.16.1 Fault Tolerance

Fault-tolerance is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. The basic characteristics of fault tolerance require:

1. No single point of failure.
2. No single point of repair.
3. Fault isolation to the failing component.
4. Fault containment to prevent propagation of the failure.
5. Availability of reversion modes.

In addition, fault tolerant systems are characterized in terms of both planned service outages and unplanned service outages. These are usually measured at the application level and not just at a hardware level. The figure of merit is called availability and is expressed as a percentage. A five nines system would therefore statistically provide 99.999% availability. A spare component addresses first fundamental characteristic of fault-tolerance in three ways:

(i) Replication: Providing multiple identical instances of the same system or subsystem, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum;

(ii) Redundancy: Providing multiple identical instances of the same system and switching to one of the remaining instances in case of a failure (failover);

(iii) Diversity: Providing multiple *different* implementations of the same specification and using them like replicated systems to cope with errors in a specific implementation.

5.16.2 Redundant Array of Inexpensive Disks (RAID)

RAID provides fault tolerance and performance improvement via hardware and software solutions. It breaks up the data to write it in multiple disks to improve performance and / or save large files. There are many methods of RAID which are categorized into several levels. There are various combinations of these approaches giving different trade -offs of protection against data Loss, capacity, and speed.

RAID levels: Levels 0, 1, and 5 are the most commonly found, and cover most requirements. Generally, most organisations use RAID-1and RAID-5 for data redundancy.

Electronic vaulting: Electronic vaulting is a backup type where the data is backed up to an offsite location. The data is backed up, generally, through batch process and transferred through communication lines to a server at an alternate location.

Remote journaling: Remote journaling is a parallel processing of transactions to an alternate site, as opposed to batch dump process like electronic vaulting. The alternate site is fully operational at all times and introduces a very high level of fault tolerance.

Database shadowing: Database shadowing is the live processing of remote journaling but creates even more redundancy by duplicating the database sites to multiple servers.

5.17 Testing of BCP

The effectiveness of BCP has to be maintained through regular testing. The five types of tests of BCP are:

1. Checklist test
2. Structured walk through test
3. Simulation test
4. Parallel test
5. Full interruption test

1. Checklist test: In this type of test, copies of the plan are distributed to each business unit's management. The plan is then reviewed to ensure that the plan addresses all procedures and critical areas of the organisation. In reality, this is considered as a preliminary step to real test and is not a satisfactory test in itself.

2. Structured walk through test: In this type of test, business unit management representatives meet to walk through the plan. The goal is to ensure that the plan accurately reflects the organisation's ability to recover successfully, at least on paper. Each step of the plan is walked through in the meeting and marked as performed. Major faults with the plan should be apparent during the walkthrough.

3. Simulation test: In this type of test, all of the operational and support personnel who are expected to perform during an actual emergency meet in a mock practice session. The

objective is to test the ability and preparedness of the personnel to respond to a simulated disaster. The simulation may go to the point of relocating to the alternate backup site or enacting recovery procedures but does not perform any actual recovery process or alternate processing.

4. Parallel test: A Parallel test is a full test of the recovery plan, utilizing all personnel. The difference between this and the full interruption test is that the primary production processing of the business does not stop, the test processing runs in parallel to the real processing. The goal of this type of test is to ensure that critical systems will actually run at the alternate processing backup site. Systems are relocated to the alternate site, parallel processing backup site, and the results of the transactions and other elements are compared. This is the most common type of disaster recovery plan testing.

5. Full interruption test: During a full interruption test, a disaster is replicated event the point of ceasing normal production operations. The plan is implemented Asif it was a real disaster, to the point of involving emergency services. This is a very severe test, as it can cause a disaster on its own. It is the absolute best way to test a disaster recovery plan, however, because the plan either works or doesn't.

Documentation of results: During every phase of the test, a detailed documentation of observations, problems and resolutions should be maintained. This documentation can be of great assistance during an actual disaster. They are also helpful in improving and maintaining the plan as they reveal the strengths and weaknesses of the plan. No test is ever a failure because, however badly it may seem to have gone lessons can still be learnt from it. However, it should be remembered that if a test is not planned properly, it could actually create a disaster. Live tests especially could create disaster if not planned properly because they use real people and real resources in real conditions, probably during normal working hours. Live tests should only be considered after the BCP has been tested in full and all Recovery Team members fully trained. The worst way to test a Plan is to turn off the power suddenly, for example, and tell people to exercise their Recovery Plans, the interruption and delay to normal work could well become a disaster in itself.

Results Analysis: The results of each test should be recorded to identify:

I. What happened;

II. What was tested successfully; and

III. What needs to be changed?

If a test indicates that the BCP needs to be changed, the change should be made, and the test repeated until all aspects are completed satisfactorily. When all the components have been tested satisfactorily, the whole BCP is ready for testing. It should not be assumed that because the components work individually there is no need to test the whole BCP. Putting it all together may reveal problems which did not show up in lower level testing. When preparing for testing, the participants should be given all the information and instruction they need.

5.18 BCP Audit and Regulatory Requirements

Business Continuity Planning (BCP) refers to ability of organisations to recover from a disaster and continue operations with least impact. It is imperative that every organisation whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the organisation. It is not enough that organisation has a BCP, but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the organisation.

5.18.1 Role of IS Auditor in BCP Audit

In a BCP Audit, the IS auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP review is to assess the ability of the organisation to continue all critical operations during a contingency and recover from a disaster within the defined critical recovery time period. IS Auditor is expected to identify residual risks which are not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit. BCP of an organisation is also to be reviewed to a limited extent for the assessment of an auditee organisation from the perspective of going concern.

5.18.2 Regulatory Requirements

A business continuity plan audit should provide management an evaluation of the organisation's preparedness in the event of a major business disruption. It should identify issues that may limit interim business processing and restoration of same. It should also provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans. The business continuity plan audit should be programmed to cover the applicable laws, standards and Frameworks etc. Understanding of the applicable Regulatory requirements are essential while doing the audit of any BCP environment to ensure whether the information technology arrangement related to Business continuity and disaster recovery plans are in conformity with the applicable Laws and regulations. It is also necessary to understand whether the information technology related to BCP/DRP arrangements are supporting the business compliance with external laws and regulations. Hence before designing the audit scope and programs all external compliance requirements are to be identified and External compliance requirements are adequately addressed.

5.18.3 Regulatory Compliances of BCP

Regulatory requirements play an important role in outlining the need for BCP for organisations which provide critical services. These regulations also provide generic guidelines for

implementing BCP. Some of the sample laws and regulations that are applicable are given here:

5.18.3.1 Basel Committee on E Banking

The Basel Committee on E-Banking outlines the principles for electronic banking as; "Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services". The Committee underlines that banks should also ensure that periodic independent internal and/or external audits are conducted about business continuity and contingency planning. These requirements are spelt out in Appendix VI relating to "Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking":

5.18.3.2 Indian legislations

There are various Indian legislations such as the Information Technology Act, Indian Income Tax act, Goods and Services Tax Act etc. which require data retention for specific number of years. Organisations which have to comply with these requirements have to ensure that they have a proper business continuity plan which meets these requirements. The Reserve bank of India provides regular guidelines to financial institutions covering various aspects of IT deployment. These guidelines cover business continuity and disaster recovery procedures for various types of business operations which are dependent on I&T environment.

Bank Audit

The Long Form Audit report in the case of statutory audit of banks contains two key points relating to business continuity and disaster recovery which need to be evaluated and commented by the statutory auditor.

- Whether regular back-ups of accounts and off-site storage are maintained as per the guidelines of the controlling authorities of the bank?
- Whether adequate contingency and disaster recovery plans are in place for loss/encryption of data?

The first point may be irrelevant in case of audit of branches where core banking solution is implemented. However, a general review of the contingency and disaster recovery plans has to be made by auditor and required comments provided. In case of internal audit or concurrent audit of banks, there are specific areas of BCP which need to be reviewed by the auditors.

5.19 ISO 22301:2019

ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements is an international standard published by the International Organization for Standardization (ISO), and it describes how to manage business continuity in an organization.

The focus of ISO 22301 is to ensure continuity of business delivery of products and services after occurrence of disruptive events (e.g., natural disasters, man-made disasters, etc.). This

is done by finding out business continuity priorities (through business impact analysis), what potential disruptive events can affect business operations (through risk assessment), defining what needs to be done to prevent such events from happening, and then defining how to recover minimal and normal operations in the shortest time possible (i.e., risk mitigation or risk treatment). Therefore, the main philosophy of ISO 22301 is based on analyzing impacts and managing risks: find out which activities are more important and which risks can affect them, and then systematically treat those risks.

The strategies and solutions that are to be implemented are usually in the form of policies, procedures, and technical/physical implementation (e.g., facilities, software, and equipment). In most cases, organizations do not have all the facilities, hardware, and software in place – therefore, ISO 22301 implementation will involve not only setting organizational rules (i.e., writing documents) that are needed in order to prevent disruptive incidents, but also developing plans and allocating technical and other resources to make the continuity and recovery of business activities possible.

5.20 ISO 27031:2011

ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

5.21 Services that can be Provided by an IS Auditor in BCM

1. Management Consultancy Services in providing guidance in drafting of a BCP/DRP. CAs can provide insight to the organisation on the development of a BCP/DRP. Appropriate guidance in drafting a BCP such as scoping of the BCP as per the policy etc. Development of a BCP Manual.
2. Management Consultancy Services in designing and implementing a BCP/DRP. CAs can provide guidance in the actual design of the BCP that is relevant to the organisation’s nature and size. They can assist the management in implementing the

BCP in the organisation. They can design the phases for implementation of the BCP and thus ensure correct and effective implementation of the BCP in the organisation.

3. Designing Test Plans and Conducting Tests of the BCP/DRP. CAs can design plans that can be used by the management for regular testing of the BCP. He can also evaluate the tests that have been conducted by the management.
4. Consultancy Services in revising and updating the BCP/DRP. Maintenance of the BCP is a periodic process. Technologies evolve, and the Business Environment often changes and hence it is necessary to revise and update the BCP.
5. Conducting Pre-Implementation Audit, Post Implementation Audit, General Audit of the BCP/DRP.
   A Chartered Accountant can provide assurance whether the BCP would suffice to the organisation.
6. Consultancy Services in Risk Assessment and Business Impact Analysis. Conducting a proper Business Impact Analysis and assessing the risks that are present in the organisation's environment is really crucial for the correct development of the BCP/DRP. CAs can help in the development stages by conducting BIA and Risk Assessment for the organisation.
7. CAs can be involved in any/all areas of BCP implementation or review. These areas could be pertaining to:
   (a) Risk Assessment
   (b) Business Impact Assessment
   (c) Disaster Recovery Strategy Selection
   (d) Business Continuity Plan Development
   (e) Fast-track Business Continuity Development
   (f) BCP / DRP Audit, Review and Health-check Services
   (g) Development and Management of BCP / DRP Exercises and Rehearsals
   (h) Media Management for Crisis Scenarios
   (i) Business Continuity Training

5.22 Summary

This chapter has provided an overview of the key concepts relating to management of BCP, DRP and Incident Responses. Together, these are to be implemented as part of Business Continuity management. The ultimate objective of a BCM is to recover from a crisis as fast as possible and at the lowest possible cost. The development of a Business Continuity Plan can be done with the support of BCP Policy existing in an organisation. BCP Policy sets the scope

of the plan. Development of BCP involves planning BCP as a project includes conducting a Business Impact Analyses, Risk Assessment, testing of the BCP, providing training and awareness and continuous maintenance of the BCP Plan. IS Auditor having to understand BCP processes and key activities for each of the key processes. This chapter has provided an overview of the BCP processes. Audit Process that are to be followed by an IS Auditor. A control is placed always against an identified risk by the management. It is essential for an IS Auditor to verify the controls that have been put in place by the management for adequacy and existence.

5.23 Questions

1. Which of the following is MOST important to have in a disaster recovery plan?
   A. Backup of compiled object programs
   B. Reciprocal processing agreement
   C. Phone contact list
   D. Supply of special forms
2. Which of the following BEST describes difference between a DRP and a BCP? The DRP:
   A. works for natural disasters whereas BCP works for unplanned operating incidents such as technical failures.
   B. works for business process recovery and information systems whereas BCP works only for information systems.
   C. defines all needed actions to restore to normal operation after an un-planned incident whereas BCP only deals with critical operations needed to continue working after an un-planned incident.
   D. is the awareness process for employees whereas BCP contains procedures to recover the operation?
3. The MOST significant level of BCP program development effort is generally required during the:
   A. Early stages of planning.
   B. Evaluation stage.
   C. Maintenance stage.
   D. Testing Stage.
4. An advantage of the use of hot sites as a backup alternative is:
   A. The costs related with hot sites are low.

B. That hot sites can be used for a long amount of time.

C. That hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.

D. That hot sites can be made ready for operation within a short span of time.

5. All of the following are security and control concerns associated with disaster recovery procedures EXCEPT:

A. Loss of audit trail.

B. Insufficient documentation of procedures.

C. Inability to restart under control.

D. Inability to resolve system deadlock.

6. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up onto tape. During the backup procedure, the disk drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?

A. The previous day's backup file and the current transaction tape

B. The previous day's transaction file and the current transaction tape

C. The current transaction tape and the current hardcopy transaction log

D. The current hardcopy transaction log and the previous day's transaction file

7. An IS auditor reviewing an organisation's information systems disaster recovery plan should verify that it is:

A. Tested every 1 month.

B. Regularly reviewed and updated.

C. Approved by the chief executive officer

D. Approved by the top management

8. Which of the following offsite information processing facility conditions would cause an IS auditor the GREATEST concern?

A. Company name is clearly visible on the facility.

B. The facility is located outside city limits from the originating city.

C. The facility does not have any windows.

D. The facility entrance is located in the back of the building rather than the front.

9. Which of the following methods of results analysis, during the testing of the business continuity plan (BCP), provides the BEST assurance that the plan is workable?

A. Quantitatively measuring the results of the test

B. Measurement of accuracy

C. Elapsed time for completion of prescribed tasks

D. Evaluation of the observed test results

5.24 Answers and Explanations

1. A. Of the choices, a backup of compiled object programs is the most important in a successful recovery. A reciprocal processing agreement is not as important, because alternative equipment can be found after a disaster occurs. A phone contact list may aid in the immediate aftermath, as would an accessible supply of special forms, but neither is as important as having access to required programs.

2. C. The difference pertains to the scope of each plan. A disaster recovery plan recovers all operations, whereas a business continuity plan retrieves business continuity (minimum requirements to provide services to the customers or clients). Choices A, B and D are incorrect because the type of plan (recovery or continuity) is independent from the sort of disaster or process and it includes both awareness campaigns and procedures.

3. A. A company in the early stages of business continuity planning (BCP) will incur the most significant level of program development effort, which will level out as the BCP program moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS Auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

4. D. Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution and does require that equipment and systems software be compatible with the primary installation being backed up.

5. D. The inability to resolve system deadlock is a control concern in the design of database management systems, not disaster recovery procedures. All of the other choices are control concerns associated with disaster recovery procedures.

6. A. The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

7. B. The plan must be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel, otherwise it may quickly become out of date and may no longer be effective (for example, hardware or software changes in the live processing environment are not reflected in the plan). The plan must be subjected to regular testing, but the period between tests will depend on nature of the organisation and relative importance of IS. Three months or even annually may be

appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally, or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. the IS disaster recovery plan will usually be a technical document and relevant to IS and communications staff only.

8. A. The offsite facility should not be easily identified from the outside. Signs identifying the company and the contents of the facility should not be present. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from malicious attack. The offsite facility should not be subject to the same natural disaster that affected the originating site. The offsite facility must also be secured and controlled just as the originating site. This includes adequate physical access controls such as locked doors, no windows and human surveillance.

9. A. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices B and C are also quantitative, they relate to specific areas or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.

Appendix 1
Checklist and Control Matrix

Appendix 1: Checklist for a Business Continuity Plan and Audit

Process Objectives:

- To seamlessly recover from the disaster situation.
- To reduce the impact of the damage of the assets, in turn reducing the data loss.
- To assure compliances
- To sustain operations so that customer service and corporate image can be maintained.

Using this Checklist:

This checklist is to be used by the IS Auditor who is conducting the BCP Audit. This checklist covers the entire BCP Process, but it has to be customized as per the specific needs of the assignment. An IS Auditor can use this checklist as a basis for recording observations and for collecting evidences for the Audit engagement. This checklist is an illustrative example as to how an IS Auditor could conduct a BCM Audit at an organisation. It can be taken as a base for conducting such audit engagements.

Policy and Procedure	
1.	Is business continuity plan documented and implemented?
2.	Whether the scope and objectives of a BCP are clearly defined in the policy document? (Scope to cover all critical activities of business. Objectives should clearly spell out outcomes of the BCP)
3.	Whether there exist any exceptions to the scope of BCP i.e. in terms of location or any specific area, and whether the management has justifications for exclusion of the same.
4.	What is the time limit for such exclusion and what is the current strategy of covering such exclusions
5.	Are the policy and procedure documents approved by the Top Management? (Verify sign off on policy and procedure documents and budget allocations made by the management for a BCP)
6.	Does the business continuity plan ensure the resumption of IS operations during major information system failures? (Verify that the IS disaster recovery plan is in line with strategies, goals and objectives of corporate business continuity plan).

7.	Are users involved in the preparation of business continuity plan? (Managerial, operational, administrative and technical experts should be involved in the preparation of the BCP and DRP).
8.	Does the policy and procedure documents include the following? List of critical information assets. List of vendors for service level agreements. Current and future business operations. Identification of potential threats and vulnerabilities. Business impact analysis. Involvement of technical and operational expert in preparation of BCP and Disaster recovery plans. Recovery procedure to minimize losses and interruptions in business operations. Disaster recovery teams. Training and test drills. Compliance with statutory and regulatory requirements
9.	Are the BCP policy and procedures circulated to all concerned? (Verify availability and circulation of the BCP & DRP to all concerned, including onsite and offsite storage).
10.	Is the business continuity plan updated and reviewed regularly? (Verify minutes of meeting where policy and procedures are reviewed. Verify amendments made to the policy and procedure documents due to the change in business environment).
Risk Assessment	
1.	Has the management identified potential threats/vulnerabilities to business operations? (Verify the business environment study report. Risk Assessment Report?)
2.	Are the risks evaluated by the Management? (Verify the probability or occurrence of the threat / vulnerability review carried out by the management).
3.	Has the organisation selected the appropriate method for risk evaluation?
4.	Has the organisation carried out the assessment of internal controls? (Verify the internal controls mitigating the risk).
5	Has the organisation taken an appropriate decision on the risks identified? (Verify the decision-making on the options - accepted, reduced, avoided or transferred – for the risks identified).

6.	Is the risk assessment carried out at regular interval? (Verify the review frequency.)
Business Impact Analysis	
1.	Does the organisation carry out business impact analysis (BIA) for business operations?
2.	Has the organisation identified a BIA team?
3.	Are RTO and RPO defined by the management?
4.	Whether the SDO has been defined based upon RTO & RPO
5.	Whether the organisation has measured BIA? (Impact of risks on business operations can be measured in the form of business loss, loss of goodwill etc.)
6.	Is the business impact analysis carried out at a regular interval?
Development and Implementation of the BCP and DRP	
1.	Has the organisation prioritized recovery of interrupted business operations? (Prioritization of activities is based on RTO and RPO)
2.	Has the organisation identified the various BCP and DRP Teams? (Verify employees are identified, informed and trained to take an action in the event of disaster).
3.	Are the responsibilities for each team documented? (Verify the roles and responsibilities assigned to employees for actions to be taken in the event of incident/disaster)
4.	Does the BCP document(s) include the following? Scope and objective. Roles and responsibilities of BCP and DRP Teams. Incident declaration. Contact list. Evacuation and stay-in procedure. Activity priorities. Human resource and welfare procedure. Escalation procedures. Procedure for resumption of business activities. Media communication. Legal and statutory requirements. Backup and restore procedures. Offsite operating procedures

5.	Are the copies of up-to-date BCP Documents stored offsite?
6.	Does the offsite facility have the adequate security requirements? (Verify the logical access, physical access and environmental control of the offsite).
7.	Does the BCP include training to employees? (Verify the evidences of training given).
8.	Whether the organisation has an adequate media and document backup and restoration procedures? (Verify the backup and restoration schedules adopted by the organisation)
9.	Are logs for backup and restoration maintained and reviewed? (Verify the logs maintained and review of the same by an independent person).
10.	Whether the media library has an adequate access control? (Verify the physical and logical access controls to the media library).
11.	Are the BCP and DRP communicated to all the concerned? (Verify availability and circulation of BCP & DRP to all concerned, including Onsite and offsite storage).
Maintenance of BCP and DRP	
1.	Whether the business continuity plan is tested at regular interval?
2.	Has the organisation reviewed the gap analysis of testing results? (Review process that includes a comparison of test results to the planned results).
3.	How has the organisation decided to reduce the gaps identified, what is the time limit set for addressing the same?
4.	Has the organisation got a testing plan? (Verify copy of test plan and updates).
5.	Are test drills conducted at appropriate intervals?
6.	Do organisation documents and analyses have testing results? (Verify the corrective copies of test results and analysis of the report).
7.	Has the organisation prepared action points to rectify the testing results? (Verify the corrective action plan for all problems encountered during the test drill).
8.	Does the organisation carry out retesting activity for action points? (Verify the evidences of retesting activities).
9.	Does the organisation review the BCP and DRP at regular intervals?
10.	Whether a review of the BCP includes following? BCP policy and procedure

	Scope and exclusion of BCP Inventory of IS assets Validating assumption made while risk assessment and preparation of BCP and DRP Risk assessment Business impact analysis Back up of system and data Training to employees Test drills

Appendix 2
Sample of BCP Audit Finding

Max Infotech should have an alternate disaster recovery site and documented procedures and policies for disaster recovery.

Observation

Max Infotech does not have an alternate disaster recovery site. Also documented Disaster Recovery Plan (DRP) and business continuity plan are not there.

Exposure

The DRP is a key plan ensuring availability of resources critical to the business operations. In the absence of documented procedures and policies for the same, it may be difficult to recover from a disaster resulting in non-availability of data and applications to the users for unacceptable period of time thereby interrupting business processes and impacting the business.

Cause

This is due to lack of documented Disaster Recovery Plan (DRP).

Recommendation

Ensure that the Max Infotech has an alternate disaster recovery site and a documented procedures and policies for disaster recovery. This document should include:

- Provision for back up and restoration of resources identified as critical to recovery;
- Provision for back up and off-site location of non-critical application software, data files and system software to facilitate their restoration following the recovery of critical application;
- Frequency of back up and off-site rotation and number of generations maintained, of production data files including databases;
- Back up and off-site copies of system software, updated or replaced with each upgrade or revision;
- Off-site copies of systems, program, user and operations documentation updated to reflect system revision;

Instructions on how to restore from back-up copies of program and data files.

Notes

Notes